C 73/3

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

National Institute of Justice / *Issues and Practices*

Dedicated Computer Crime Units

J 28.23:

READEX FICHE best copy available

About the National Institute of Justice

The National Institute of Justice is a research branch of the U.S. Department of Justice. The Institute's mission is to develop knowledge about crime, its causes and control. Priority is given to policy-relevant research that can yield approaches and information that State and local agencies can use in preventing and reducing crime. The decisions made by criminal justice practitioners and policymakers affect millions of citizens, and crime affects almost all our public institutions and the private sector as well. Targeting resources, assuring their effective allocation, and developing new means of cooperation between the public and private sector are some of the emerging issues in law enforcement and criminal justice that research can help illuminate.

Carrying out the mandate assigned by Congress in the Justice Assistance Act of 1984, the National Institute of Justice:

- Sponsors research and development to improve and strengthen the criminal justice system and related civil justice aspects, with a balanced program of basic and applied research.
- Evaluates the effectiveness of justice improvement programs and identifies programs that promise to be successful if continued or repeated.
- Tests and demonstrates new and improved approaches to strengthen the justice system, and recommends actions that can be taken by Federal, State, and local governments and private organizations and individuals to achieve this goal.
- Disseminates information from research, demonstrations, evaluations, and special programs to Federal, State, and local governments, and serves as an international clearinghouse of justice information.
- Trains criminal justice practitioners in research and evaluation findings, and assists practitioners and researchers through fellowships and special seminars.

The Director of the Institute is appointed by the President of the United States, and upon confirmation by the Senate, serves at the President's pleasure. The Director establishes the research and development objectives of the Institute. The Director has final authority to approve grants, contracts, and cooperative agreements, and maintains responsibility for fiscal operations of the Institute. In establishing its research agenda, the Institute is guided by the priorities of the Attorney General and the needs of the criminal justice field. The Institute actively solicits the views of police, courts, and corrections practitioners as well as the private sector to identify the most critical problems and to plan research that can help resolve them.

James K. Stewart

Director

U.S. Department of Justice
National Institute of Justice
Office of Communication and Research Utilization

Dedicated Computer Crime Units

by
J. Thomas McEwen

Report Contributors
Dennis Fester
Hugh Nugent

June 1989

Issues and Practices in Criminal Justice is a publication of the National Institute of Justice. Designed for the criminal justice professional, each *Issues and Practices* report presents the program options and management issues in a topic area, based on a review of research and evaluation findings, operational experience, and expert opinion in the subject. The intent is to provide criminal justice managers and administrators with the information to make informed choices in planning, implementing and improving programs and practice.

Prepared for the National Institute of Justice, U.S. Department of Justice, by Institute for Law and Justice, Inc. under contract number OJP-85-C-006. Points of view or opinions stated in this document are those of the authors and do not necessarily represent the offical position or policies of the U.S. Department of Justice. Authors are J. Thomas McEwen, Dennis Fester and Hugh Nugent of the Institute for Law and Justice, Alexandria, VA.

National Institute of Justice
James K. Stewart
Director

Program Monitor

Jonathan Budd
National Institute of Justice
Washington, D.C.

The Assistant Attorney General, Office of Justice Programs, coordinates the activities of the following program Offices and Bureaus: National Institute of Justice, Bureau of Justice Statistics, Bureau of Justice Assistance, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime.

Foreword

With the virtual explosion of technological advances in the 1980's, computers and their applications have become an integral and indispensable part of our society and its institutions. Computers were found in one home in a hundred at the beginning of the decade – by 1987 one in five households had them. Today they are as common a business tool as the ledger or the cash register. Given this dramatic increase in the use and accessibility of computers in the home and in business, it is not surprising to see an increase in the use of computers in the commission of crime.

Law enforcement faces new challenges as it seeks to strengthen capabilities for successfully investigating and prosecuting computer crime into the 1990's. Use of computers has proliferated not only in traditional crimes of theft such as embezzlement and fraud; increasingly, drug rings, prostitution rings, child pornographers and pedophiles have turned to computers to facilitate their illicit operations just as legitimate businesses do. Police say they arrive at the scene of these criminal networks and discover computers in operation.

Detectives and prosecutors realize that if law enforcement is to make greater inroads in investigating and prosecuting these types of cases, they need to become conversant with computer operations. In fact, the 1986 National Assessment Program Survey conducted by the National Institute of Justice found that 65 percent of the police chiefs and sheriffs sampled considered approaches for handling computer crime to be a high priority for further research and information sharing.

As part of its response to this need, the National Institute of Justice has published this *Issues and Practices* report, which examines in detail special units set up by local jurisdictions to handle computer crime cases. These units are staffed by investigators whose time is devoted primarily to the investigation of computer-related crimes. At present, this approach to the computer crime problem is being utilized by relatively few jurisdictions. This report should prove invaluable for jurisdictions considering or planning such a unit. Regardless of approaches used for handling computer-related crime, however, the report provides a wealth of useful information.

Two companion volumes, *Computer Crime: Criminal Justice Resource Manual* and *Organizing for Computer Crime Investigation and Prosecution,* are other important parts of NIJ's effort to provide information and ideas law enforcement can use in meeting the challenges posed by computer crime.

The proud history of law enforcement in the United States has been marked by a remarkable capacity to successfully confront and overcome new challenges. With the publication of these volumes, the National Institute of Justice hopes to assist law enforcement and prosecutorial efforts to meet the challenges they face combating crime in the computer age.

James K. Stewart
Director
National Institute of Justice

Acknowledgments

This report is about the experiences of local police and prosecutors in their investigations of computer crimes. It could not have been completed without the excellent cooperation of many investigators and prosecutors across the country. Acknowledgment is given especially to the following specialized units which are the primary focus of this report:

Alameda County, California
District Attorney's Office
High Tech Crime Team
Mr. Don Ingraham
Investigator Al Salerno

Baltimore County, Maryland
Police Department
Economic/Computer Crime Unit
Investigator Frank Simmons
Investigator Calvin Lane

Illinois State Police
Computer Crime Unit
Sgt. Abigail Abraham

Los Angeles, California
Police Department
Computer Crime Unit
Sgt. James Black

Maricopa County, Arizona
Sheriff's Department
Technical Crimes Investigation
Sgt. Bill Nibouar

San Jose, California
Police Department
High Technology Detail
Sgt. Don Brister
Sgt. David Flory
Officer Jim Aguirre

Santa Clara, California
Police Department
Fraud Unit
Sgt. Jerry Marcelli
Sgt. Pete Pearson

Santa Clara County, California
District Attorney's Office
High Technology Unit
Deputy D.A. Ken Rosenblatt

Tarrant County, Texas Office of
the Criminal District Attorney
Economic Crimes Section
Asst. Criminal D.A. Davis McCown

Many other people contributed to our understanding of computer crimes and how local agencies should approach the difficult task of organizing and training personnel for these investigations. Particular thanks go to Mr. Wayne Cerow, Cerow Investigations and Consultants, Phoenix, Arizona; Mr. Carlton Fitzpatrick, Federal Law Enforcement Training Center, Glynco, Georgia; Mr. Ken McLeod, Comsec, Inc., Phoenix, Arizona; Ms. Gail Thackery, Arizona

Attorney General's Office; Sgt. Dan Pasquale, Fremont, California, Police Department; Mr. Charles Stevens, FBI Academy, Quantico, Virginia; Honorable Douglas Southard, Municipal Court, San Jose, California; and Mr. Steve Purdy, U.S. Secret Service.

The idea for this publication began with the results from a survey of police chiefs and sheriffs conducted under the National Assessment Program at the National Institute of Justice (NIJ). Survey respondents rated computer crime as a high priority for training and research. Based on these results, Mr. Jonathan Budd, a staff member of NIJ's Research Applications and Training Division, recommended that a report be prepared on this subject. The recommendation was strongly endorsed by Ms. Virginia Baldau, Division Director; and Mr. Paul Cascarano, Assistant Director of NIJ. We greatly appreciate their support for this publication.

Table of Contents

Foreword iii

Acknowledgments v

Introduction

Computer Crime in Today's Computer Society xi
The Computer Revolution xi
Project Methodology xii
Organization of the Report xiii
Related Reports xiv

Chapter 1. An Overview of Computer Crime

Defining Computer Crime 1
Types of Computer Crimes 2
The Level of Computer Crime 5
Federal, State, and Local Responses to Computer Crimes 7
Federal Responses 7
State Responses 7
Local Responses 8

Chapter 2. Computer Crime Investigative Units

Introduction 11
Individual Computer Crime Units 13
Alameda County, California District Attorney's Office 13
Baltimore County, Maryland Police Department Economic/Computer Crime Unit 14
Illinois State Police Computer Crime Section 16
Los Angeles, California Police Department Computer Crime Unit 17
Maricopa County, Arizona Sheriff's Office Technical Crimes Investigation Unit 19
Santa Clara County, California Units 20

Tarrant County, Texas Office of the Criminal District Attorney Economic Crimes Section....21
District Attorney's Technology Theft Association (DATTA)....22
Organizational Experiences with Dedicated Units....26
Advantages and Disadvantages of Dedicated Units....26
Responsibilities of a Computer Crime Unit....28
Requirements for a Computer Crime Unit....29

Chapter 3. Computer Crime Investigations

Cases Investigated by the Computer Crime Units....37
Internal Computer Crimes....39
Data Destruction and Logic Bomb Case....39
Telecommunications Crimes....41
Hacker Case #1....41
Hacker Case #2....43
Telephone System Seizure....44
Illegal Access to Computer Services....45
Computer Manipulation Crimes....47
Embezzlement Case #1....47
Embezzlement Case #2....49
Support of Criminal Enterprises....50
Prostitution and Racketeering Case....50
Thefts of Hardware/software....51
Software Piracy....51
Theft of Silicon Wafers....53
Theft of Trade Secrets....53
Lessons Learned from Local Cases....54

Chapter 4. Computer Crime Legislation

Introduction....59
Strict Construction of Criminal Statutes....59
Computer Crime Cases....60
Computer Crime Statutes....64
Definitions....66
Offenses....69
Elements of Computer Crimes....70

Penalties 72
Venue 74
Civil Remedies 75
Miscellaneous Features 77
Conclusion 78

Chapter 5. The Future of Computer Crime

Reporting Trends 85
Investigations by Police Departments and Prosecutors 87
Prevention of Computer Crimes 89
Response of Computer Crime Offenders 90
Conclusions 91

Appendix A

Sting Operations for Computer Crimes 101

Appendix B

Computer Crime Statutes for Arkansas and Virginia 107

Appendix C

Search Warrant County of Maricopa, State of Arizona 117

Appendix D

Discovery Materials 125

LIST OF EXHIBITS

Exhibits

1-1 Categories of Computer Crimes 2

3-1 Summary of Cases and Charges 38

4-1 Summary of State Statutes 80

Computer Crime in Today's Computer Society

Suppose you could sit in the comfort and security of your home and, for an investment of less than $2,000 in microcomputer equipment, commit a crime with a possible gain of $25,000. Sound impossible? Not anymore. The advances in computers and telecommunications make this scenario a possibility in many jurisdictions across the country.

The Computer Revolution

Over the last twenty years a technological revolution has occurred as computers have increased in speed and capacity while decreasing in price. Computers are now an essential element of today's society. Large computers are used to track reservations for the airline industry, process billions of dollars daily for banks, manufacture products for industry, and conduct major transactions for businesses. Sales for software, telecommunications, and automated business systems are estimated to exceed $250 billion per year.[1]

At another level, the improvements in microcomputers have allowed small businesses to enter into the computer world with word processing, spreadsheets, and database management systems as the leading tools for accounting, payroll, correspondence, reports, inventory, customer lists, marketing plans, and many other applications. There are over ten million microcomputers in the workplace today with estimates of thirty-four million by 1994. Business budgets for automation are showing 25 percent devoted to microcomputer purchases, with the remainder allocated to other hardware, peripherals, software, and related items.[2] About 19 million households now contain homeworkers, and over 35 percent of these households own a personal computer.[3] Along with the introduction of microcomputers has come the requirement to have personnel who can understand and operate the applications. Positions in small businesses have been created to fill this void, and these valued employees hold the "keys to the kingdom." Their importance has increased as more applications are automated and business becomes more dependent on computers.

Microcomputers can also be found in homes for entertainment, school work, and many other activities. Secondary schools are acquiring microcomputers and providing training to students at an increasing rate. More people are becoming "computer literate" and at an earlier age than ever before.

At the same time that computers have become faster and cheaper, telecommunications have improved to allow computers to communicate with relative ease. Microcomputers can now "talk" to large mainframe computers several thousand miles away, allowing users to browse files subject only to the security constraints on the system.

While the computer age with improved telecommunications has resulted in great benefits to society, it has also created a wide variety of opportunities for illegal activities. Security systems can be compromised. Data can be changed or destroyed. Systems can be made inoperative. Long-distance telephone charges can be averted. Overt threats can be placed on systems. The challenge in today's society is to control these misuses while maintaining the tremendous advantages of computer systems.

Project Methodology

This report explores in detail how a few jurisdictions have approached their computer crime problems by establishing *dedicated units* to investigate and prosecute these offenses. Some of the units are located in police departments, some in sheriffs' offices, and some under the auspices of the prosecutors. Agencies participating in the study were as follows:

- Alameda County, California, District Attorney's Office
- Baltimore County, Maryland, Police Department
- Illinois State Police
- Los Angeles, California, Police Department
- Maricopa County, Arizona, Sheriff's Department
- Santa Clara County, California
  - San Jose Police Department
  - Santa Clara Police Department
  - Santa Clara County District Attorney's Office
- Tarrant County, Texas, Office of the Criminal District Attorney

These agencies have a common organizational feature: each has a unit that has been staffed with investigators who devote the majority of their time to crimes in which a computer has played an essential role.

The units were located after an extensive telephone survey that included calls to approximately 40 agencies including major police departments, prosecutors' offices, federal agencies, universities, research organizations, private investigation companies, and other groups with knowledge about computer crime investigations. The agencies listed above were the *only local agencies* found to have dedicated units for computer crime investigations.

From visits to these units, it was possible to get a clearer understanding of computer crimes and the inherent difficulties in reporting, investigating, and prosecuting these offenses. With most units, the caseloads were low when they first started, but reports increased substantially as they made their presence known to businesses and other groups. The result has been that every unit now

has more cases than it can adequately handle. There is, however, unanimous agreement that computer crime offenses are still underreported by a great extent.

It is also clear that computer crimes require more time to investigate and require different training than other types of offenses. Compared to other white-collar crimes, these cases have more technical complexities due to the involvement of computers in the offense. Training in subjects such as systems analysis, operating systems, computer programming, application software, and computer hardware is needed to become a proficient investigator of complex computer crimes.

Prosecutors are becoming more familiar with computer crimes as the numbers of reports and investigations increase. In most cases, the computer crime charges are included along with charges such as embezzlement and fraud. In a few instances, usually involving major destruction of data on systems, the computer crimes themselves are the prosecutorial focus. Prosecutors also note problems in presenting technical evidence in a simple and understandable manner to judges and jurors who are generally unfamiliar with computers. Prosecutors expect computer crime cases to increase in the future, and more court cases will undoubtedly result.

Further information on all these areas is provided in the chapters of this report. The experiences of the participating units have been used to illustrate the special nature of these crimes.

Organization of the Report

- **Chapter 1** gives an overview of computer crime, including estimates of the increases in computer crimes and specific examples like the crime at the start of this chapter.
- **Chapter 2** describes the units that are the focus of this study, including the backgrounds, training, responsibilities, and caseloads of the investigators. In addition, procedures for establishing a full-time unit are provided.
- **Chapter 3** presents detailed descriptions of eleven actual cases from the files of the investigative units. These cases reflect the wide range of possible computer crimes along with the investigative techniques needed to resolve them.
- **Chapter 4** is an overview of state statutes on computer crimes. The chapter gives a history of key computer crime cases, defines terms typically found in the statutes, and provides the legal language of specific offenses.
- **Chapter 5** discusses the future of computer crimes and the need for more local agencies to address the problem.

- **Several appendices** have been developed for this report. Collectively, they contain (1) a description of a "sting" operation for identifying illegal bulletin boards, (2) two state statutes on computer crimes, (3) an example of a search warrant for computer hardware and software, and (4) a discovery motion from a defendant in a complex crime case.

Related Reports

Two related studies funded by the National Institute of Justice have recently been concluded on the subject of computer crimes. One was aimed at determining how local jurisdictions *without* specialized units are responding to computer crimes.[4] Several approaches were identified including (1) regional networking for investigations, (2) use of private investigators, and (3) establishment of associations to share resources for investigations.

In another study, the *Computer Crime: Criminal Justice Resource Manual*, initially published over ten years ago, has been updated. The tremendous changes in computer technologies have created a need to provide more current information on how to investigate and prosecute these offenses.[5]

Chapter 1

An Overview of Computer Crime

Defining Computer Crime

Definitions of computer crime have changed over the years as the uses (and misuses) of computers have expanded into new areas. When computers were first introduced into businesses, computer crime was defined simply as a form of white-collar crime committed inside a computer system. This definition covered virtually all the offenses possible with computers at that time. As computer applications expanded – particularly into telecommunications – computer crimes also expanded and began to include offenses in which computers were either directly or indirectly involved in committing crimes.

The most appropriate definition for computer crime today is *any illegal act for which knowledge of computer technology is used to commit the offense.*[6] While admittedly broad, this definition covers all the offenses now associated with computers.[7] Thefts of hardware and software, manipulation of data, illegally accessing computer systems by telephone, and altering programs all fit under this definition (see Chapter 4 for a fuller discussion of the definitions of computer crimes appearing in state statutes).

Another feature of this definition is that a computer can be either actively or passively involved in an offense. Illegally changing data in a database, destroying files, and using a "hacking" program to gain access into a system are examples of active involvement of a computer. By contrast, passive involvement means that the computer is a tool in the offense, but computer crime charges may not be relevant. Thus, a narcotics case in which a database exists describing clients and distribution networks can be classified as a computer crime since a computer is used to support an illegal act.

To further illustrate the need for a broad definition, an objective of computer crime units is to reduce the incidence of all types of crimes in which computers play a role. As described in Chapter 2, computer crime investigators devote a significant amount of time to preventive activities ranging from speeches at the meetings of computer users' groups to the establishment of associations for combatting computer crimes. The aim is always to increase the awareness of computer crimes, provide guidelines for prevention, and promote the reporting of offenses when they occur.

Types of Computer Crimes

Given that computer crimes cover a variety of different illegal activities, it is beneficial, as shown in Exhibit 1-1, to classify computer crimes into categories based on common characteristics. Five categories are reflected in the exhibit:

- Internal computer crimes
- Telecommunications and telephone crimes
- Computer manipulation crimes
- Computers in support of crimes
- Thefts of hardware and software

By reviewing these groups, we can get a better understanding of the unique characteristics of computer crimes and the expertise needed to investigate and prosecute these offenses.

Exhibit 1-1
Categories of Computer Crimes

Internal Computer Crimes

- Trojan horses
- Logic bombs
- Trap doors
- Viruses

Telecommunications Crimes

- Phreaking
- Hacking
- Illegal bulletin boards
- Misuses of telephone systems

Computer Manipulation Crimes

- Embezzlements
- Frauds

Support of Criminal Enterprises

- Databases to support drug distributions
- Databases to record client information

Hardware/Software Thefts

- Software piracy
- Thefts of computers
- Thefts of microprocessor chips
- Thefts of trade secrets

Internal computer crimes are alterations to programs that result in the performance of unauthorized functions within a computer system. These offenses, usually committed by computer programmers, require an extensive amount of computer knowledge. A programmer may, for example, change an existing program so that it appears to operate normally but in fact performs unwanted functions whenever certain logical conditions are satisfied. Under these conditions, the program may erase files, change data, or cause the system to crash. Because these crimes have been around for years, they have been given names, such as *Trojan horses*, *logic bombs*, and *trap doors*, to indicate different programming techniques for performing the unauthorized functions.

Viruses, the most recent type of internal computer crime, are sets of instructions that not only perform unauthorized functions, but also secretly attach themselves to other programs. With this self-propagating process, they spread through a system and to other systems when the "infected" program is copied or transmitted. Viruses may be relatively benign, such as a virus that merely displays an innocuous message on the computer screen. More destructive viruses are possible since it is just as easy to erase files as to display a message. At the same time, the destructive instructions can be embedded in other programs which may later be executed on other systems. Since viruses appear to be here to stay, the rampant copying of programs that characterized the early days of the computer revolution are gone, and users are now urged to be much more careful in obtaining programs.

Telecommunications crimes involve the illegal access or use of computer systems over telephone lines. A *hacking* program tries to find valid access codes for a computer system by continually calling the system with randomly generated codes. With a valid code found in this manner, the system can be accessed and costs diverted to an innocent customer. Use of a hacking program constitutes unauthorized access to a system, and access codes generated by a hacking program are stolen property.

Misuses of telephone systems are another form of telecommunications crimes. *Phone phreaking* is telephone fraud carried out by electronic devices[8] that emit tones signalling normal long-distance transactions to the telephone system. These illegal devices trick the telephone system into believing that long-distance charges are being legitimately processed. Another misuse of a telephone system is to take over a telephone line for one's own advantage. In a case discussed in Chapter 3, an individual found a way to avoid the internal accountability for long-distance calls and then sold time to friends for international calls. The increased sophistication in telephone systems has not served as a deterrent from trying to find new ways of avoiding long-distance charges.

Computer manipulation crimes involve the changing of data or creation of records in a system for the specific advancement of another crime. Virtually all

embezzlements in financial institutions require the creation of false accounts or modifications of data in existing accounts in order to perform the embezzlements. The perpetrator need not know computer programming but must have a good sense of how to operate the system. The embezzlement offense will always be the main charge but computer crime charges (e.g., unauthorized access to a computer system) may also be made. These computer crimes are necessary, although not sufficient, for the real intent of the perpetrators in these cases.

Computer systems may also serve in *support of criminal enterprises*. In a case described in Chapter 3, a microcomputer system assisted the daily operations of a prostitution ring. The system is strong evidence for establishing the existence of a continuing criminal enterprise even though computer crimes have not occurred. A key feature here is that the investigators must have a good knowledge of computers in order to confiscate and analyze the systems for effective prosecutorial actions of the primary offenses.

Databases developed by illegal drug operators for tracking distribution also fall into this category. Drug arrests have been made in which the computerized information played an essential role in the conviction of the offenders. All too often, however, local police departments are ignoring the computer information either because they do not have the capabilities to analyze the computer or because they do not believe the information will be of particular value. As one investigator stated, an interesting parallel is that it took years for investigators to learn the value of confiscated notebooks in developing leads and obtaining convictions. Now the same lesson has to be learned again with computer information.

Computer bulletin boards are another source of information to support illegal activities. Bulletin boards allow for the storing of information to be retrieved by someone dialing into the system. They are usually established for a specific audience, such as boards established by computer clubs to share information among members. There are probably over 10,000 bulletin boards now in existence across the country covering virtually every subject imaginable.

There are several examples of how bulletin boards have been used in support of criminal activities. In two of the cases in Chapter 3, bulletin boards were used to relay illegally obtained access codes into computer service companies. Pedophiles have been known to leave suggestive messages on bulletin boards, and other sexually oriented messages have been found on bulletin boards. Members of cults and sects have also communicated through bulletin boards. While the storing of information on bulletin boards may not by itself be illegal, the use of bulletin boards has certainly advanced many illegal activities.

Software and hardware thefts are the final category in this typology. A common offense is *software piracy*, defined as the unauthorized copying of a proprietary package. The most blatant form of piracy occurs when someone purchases a proprietary program, makes copies, and sells the copies for profit. Stealing *trade secrets* about products under development is another type of theft. Of course, the usual reason for taking trade secrets is to market them to competing companies for personal gain. These offenses generally occur in parts of the country known for research and development of computer systems. Because these areas also manufacture computer products, *thefts of hardware*, from microcomputer chips to large mainframes, are not uncommon. While hardware and software thefts may be dismissed as merely thefts on a grander scale, they are computer crimes because the computers are the target of an illegal activity.

The Level of Computer Crime

Determining the amount of computer crime from official records is impossible because of the lack of reporting by businesses. Reasons for not reporting computer crimes include:

- A business may not want it known to clients that the computer system was compromised. Financial institutions are particularly sensitive about the potential loss of customer confidence.
- A business may not believe that the local law enforcement agency and prosecutor's office are equipped to investigate this type of offense.
- After discovering a computer crime, the business may hire a private investigator rather than going to the local police.
- A business may decide that the cost of prosecution is too much given the small likelihood of conviction or the lack of severe legal sanctions in the statutes.
- The business may determine that an employee committed the crime and take immediate action on their own. Generally, the action is to fire the employee and avoid any contact with the criminal justice system.

In spite of the reporting problems, one point of agreement among experts is that the incidence of computer crime is increasing each year. Surveys by *Security Magazine* in 1985 and 1986 support this perception.[9] One of the survey questions was "Do you believe computer crime is going undetected in your company?" A total of 19 percent responded "Yes" in 1986, compared to 7 percent in 1985. Moreover, in the 1986 survey, another 34 percent responded "Maybe" indicating that more than half at least suspect that computer crimes are going undetected in their facilities.

Other results from their survey were:

- In 1985, 13 percent of the respondents stated that their company had detected at least one computer crime in the last five years. In 1986, 18 percent responded affirmatively.
- In 1985, the value of the most recent loss due to computer crime averaged $67,000 compared to a value of $93,000 in 1986 – almost a 40 percent increase. One in five crimes was valued at more than $99,000.
- Asked how they detected their computer crimes, companies gave multiple responses. Approximately 39 percent were discovered by following tips from employees. Thirty-five percent mentioned audit trails, 32 percent through audits by an internal department, and 26 percent through investigation into suspected losses. Interestingly, 23 percent said the computer crime was detected by "chance" indicating that the companies believed they were fortunate to have discovered the crimes.
- Forty-four percent of the respondents planned to increase spending on security in the following year. The median increase among these companies was 13 percent with one in five planning increases of 30 percent or more.

Surveys conducted to determine the total monetary loss due to computer crimes have generally resulted in wide ranges on their estimates. The American Bar Association conducted a study in 1984 which concluded that annual computer crime losses were between $145 million and $730 million.[10] A more recent study by the accounting firm Ernst & Whinney in Cleveland estimated that high-tech thieves steal $3 billion to $5 billion annually in the United States alone. With regard to detection and reporting of computer crimes, another study stated that only one percent of all computer crimes are detected and only 15 percent of these are reported.

These estimates have wide ranges for several reasons. Each study has its own definition of computer crime which automatically leads to considerably different estimates. Further, no one really knows the extent to which computer crimes are underreported. Subsequently, assumptions on the degree of underreporting impact the total estimate of losses. Finally, there are inherent problems in placing monetary values on the losses from some computer crimes. Many thefts of services (for example, the personal use of a computer) are from internal company systems that do not charge for their services. Thus, no direct financial loss is incurred, and any estimate of losses is problematic. In summary, while dollar values of computer crimes can serve as an indicator of the extent of the problem, they should not be considered as precise and reliable estimates.

Federal, State, and Local Responses to Computer Crimes

Federal Responses

Federal agencies have traditionally had more involvement with computer crimes than agencies at the state and local level. Legislative authority comes specifically from Section 1029 ("Fraud and Related Activity in Connection with Access Devices") and Section 1030 ("Fraud and Related Activity in Connection with Computers") of Title 18 of the United States Code. Access devices are broadly defined in Section 1029 as "any card, plate, code, account number, or other means of account access..." used to obtain items and services of value or to initiate a transfer of funds. Punishable offenses under this section include use of unauthorized or counterfeit access devices with intent to defraud, use of device-making equipment, attempts to commit offenses with access devices, and conspiracies to commit offenses with access devices.

Section 1030 is primarily concerned with the unauthorized access of computers used by federal agencies. Provisions of this section are concerned with (1) unauthorized access that could be injurious to the United States, (2) protection of financial institution records, and (3) alteration and destruction of data in federal interest computers.[11]

The Federal Bureau of Investigation (FBI), the Internal Revenue Service (IRS), and the United States Secret Service are the primary federal agencies that have trained investigators in computer crime investigations. The IRS investigates tax evasion cases that may also involve computer systems as part of the evasion scheme. Under an agreement between the Secretary of the Treasury and the Attorney General signed in August 1985, the FBI usually has primary jurisdiction for Section 1030 cases involving bank fraud, organized crime, national security, or terrorism, while the Secret Service has joint jurisdiction over other violations.

State Responses

The recent increase in the number of states having computer crime laws is indicative of the growing concerns of legislators in this area. In 1979, only six states had computer crime statutes.[12] Today, forty-eight states have computer crime legislation (Vermont and West Virginia are the exceptions). These statutes have provided better definitions of computer crime from a legal perspective and have specified sanctions for convicted offenders (see Chapter 4 for a discussion of these statutes).

A few state agencies have become active in computer crime investigations. The Illinois State Police has a specialized computer crime unit which participated in this study. Staffed by two full-time investigators, the unit's caseload consists

primarily of telecommunications crimes occurring in the state. Their activities are described in detail in the next chapter.

The Arizona State Attorney General's Office has been particularly active in prosecuting computer crimes. Although there is no specially designated unit, one investigator and one attorney devote a considerable amount of their time to computer crime cases and are particularly active in assisting local agencies around the state in investigations. This approach to computer crime investigations is discussed in detail in a related report.[13]

Local Responses

The responses by local police departments and prosecutors' offices to computer crimes have been mixed. While some agencies have provided training to detectives on how to detect and investigate computer crimes, most agencies have not placed a special emphasis on computer crimes.

This is not to say that law enforcement agencies lack interest. In the 1986 National Assessment Program survey, conducted by the Institute for Law and Justice for the National Institute of Justice, 75 percent of the police chiefs and 63 percent of the sheriffs rated computer crime investigations as a potentially significant cause of future workload in their departments. In large jurisdictions (over 500,000 population) the responses are even higher at 84 percent for police chiefs and 75 percent for sheriffs.

Follow-up calls to selected departments indicated several reasons for this response. One is that many embezzlement and fraud cases now involve the manipulation of a computer system. While the investigation of embezzlement starts in a traditional manner by interviewing employees and gathering physical evidence, investigators eventually reach a point where knowledge of computer systems is essential to complete the case.

Police chiefs and sheriffs also report that other types of criminal activities are starting to involve computers. Narcotic traffickers have been known to maintain records on microcomputer systems. While not a computer crime, these records could be valuable to investigators in making cases and developing leads. Without computer knowledge, however, investigators may not be able to take advantage of the stored information.

In summary, there has been a natural progression of involvement in computer crimes starting with federal agencies and proceeding in recent years to state and local agencies. States have found it necessary to enact legislation dealing specifically with computer crimes and, at least in a few states, have started to emphasize enforcement of these statutes.

At the local level, many agencies have provided limited training on computer crime investigations, but only a few have placed any type of emphasis on these crimes. However, based on the survey responses just described and the anticipated increase in these offenses, it is expected that more local agencies will have to develop better resources for preventing and investigating computer crimes. Establishing dedicated units is one approach to the problem. Their experiences, as presented in the next chapter, offer valuable lessons in the establishment of these units, the necessary qualifications of investigators, their training needs, and the benefits to be derived from dedicated units.

Chapter 2

Computer Crime Investigative Units

Introduction

Identification of agencies with full-time personnel for computer crime investigations began by contacting federal agencies with similar responsibilities. One of the federal agencies called was the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia which offers training in computer crime investigations to federal, state, and local investigators. Personnel at FLETC were particularly helpful in providing the names of several local law enforcement and prosecutor agencies that had sent investigators to FLETC training over the last two years. These agencies were then contacted by telephone to determine whether they had full-time investigators for computer crimes and whether any other agencies in their area had full-time investigators.

Calls were also made to several other large police departments and prosecutors' offices with the aim of locating units devoted to computer crimes. Finally, other groups, including universities, research organizations, security associations, and private investigation companies, were contacted for suggestions on local agencies that might have specialized units. These agencies were then contacted directly for further information.

In total, approximately 40 police and prosecutor agencies were contacted directly to determine whether they had dedicated units. The nine units that are the subject of this report were identified from this process. It should be clear from the above description that the selection was approached in a systematic manner based on the recommendations of knowledgeable people in the field. These are not the only dedicated units in the country, and even during the gathering of information for this report, other agencies formed dedicated units for computer crime investigation and prosecution. In summary, these nine selected units provided a wealth of information on this approach to the computer crime problem and they certainly appear to be representative of all dedicated units.[14]

The telephone calls resulted in the identification of the units that are the topic of this chapter:

- Alameda County, California District Attorney's Office
  High Tech Crime Team
- Baltimore County, Maryland Police Department
  Economic/Computer Crime Unit
- Illinois State Police
  Computer Crime Section

- Los Angeles, California Police Department
  Computer Crime Unit
- Maricopa County, Arizona Sheriff's Department
  Technical Crimes Investigation Unit
- Santa Clara County, California
  - San Jose Police Department
    High Technology Detail (in Fraud Unit)
  - Santa Clara Police Department
    Fraud Unit
  - Santa Clara County District Attorney's Office
    High Technology Unit
- Tarrant County, Texas Office of the Criminal District Attorney
  Economic Crimes Section

Subsequent discussions with members of these agencies indicated that the units were established in different ways. In three of the jurisdictions (Baltimore County, Illinois, and Tarrant County), the management of the agencies saw a need for full-time personnel to investigate computer crimes because of the increase in reports of this nature. In three other agencies (Alameda County, Los Angeles, and Maricopa County), one or two investigators became personally interested in computer crimes as a result of isolated cases and eventually persuaded top management on the benefits of establishing a full-time unit. The Santa Clara County units are unique in that they are an outgrowth of a state-funded pilot project called the District Attorney's Technology Theft Association (DATTA). Located in Santa Clara County, DATTA was aimed at bringing law enforcement investigators, prosecutors, and the business community together for a concerted effort to prevent high technology crimes. The successes of DATTA resulted in a keener awareness of computer crimes throughout the state and more coordination of criminal justice and business in the prevention and investigation of computer crimes.

The following section describes each of these units in detail including the qualifications of the investigators, their training, caseloads, overall responsibilities, and other relevant information. After this section is a discussion of the DATTA organization with information on how it was established, what it has achieved, and the impact it currently has on computer crime investigations in California. The final section describes the organizational experiences with specialized units including the advantages and disadvantages of these units, their usual responsibilities, and the steps generally taken to establish them. Ideas in this section were generated from discussions with the personnel in the participating agencies on such topics as the talents of investigators needed for computer crimes, training needs, and hardware and software requirements.

Individual Computer Crime Units

Alameda County, California District Attorney's Office

Because Alameda County has long been one of the centers for hardware and software development, the District Attorney's Office has been involved in computer crimes for many years. One of the attorneys is a nationally recognized expert in computer crime investigations who prosecuted his first computer crime case in 1974 and has personally handled many more cases since that time. He has also been instrumental in developing the legislation in California on computer crimes. His involvement in computer crimes has kept this office at the forefront of these investigations.

As noted by this attorney, the nature of computer crimes has changed considerably in the county over the last ten years. The evolution of microcomputers has created more opportunities for computer crimes. Microcomputers appear in the majority of computer crime cases handled by this office. As a consequence, there is a greater need for law enforcement agencies and attorneys in the county to understand "data preservation" for evidentiary purposes. Another trend in Alameda County is that more defense attorneys are becoming proficient in computer crime statutes. The expectation is that more cases will be going to trial and more attorney time will be required for prosecution.

Because of these changes, the basic philosophy at the District Attorney's Office is that any attorney in the office should be able to handle a computer crime case. The prosecutor most familiar with computer crimes has personally trained many of the other attorneys in the office. Several now have enough knowledge in computer crime laws to handle cases without assistance. In 1987, the attorneys in the office filed 30 specific computer crime charges in their cases.

Another member of the office is an investigator (not an attorney) who spends the majority of his time on computer crime cases. This individual has handled many computer crimes including embezzlements, frauds, hacking, and misuses of telephone systems. On an annual basis, this investigator is involved in approximately 35 computer crime cases.

There are many uses of his technical expertise. Through a search warrant, a system can be brought into the office if it is believed that the system is an "instrument to the crime." In these instances, the investigator will check the system and determine what information can be obtained from it. In addition, he serves as an important resource for law enforcement agencies in the county. Many of these agencies do not have the necessary expertise for computer crime cases and enlist the investigator for technical expertise. This approach has the dual advantage of assisting the departments and involving someone from the district attorney's office at the beginning of a case.

These two individuals form a "High Tech Crime Team" for the office. Their primary function is to investigate and prosecute major computer crime cases.

On large complex cases, the team may be part of a task force drawn from different sections of the office. This overall team approach takes advantage of the specialized skills of several attorneys. Aspects of these cases related to computers will, of course, be handled by the High Tech Crime Team.

In summary, the Alameda County District Attorney's Office is one of the most active in the country in developing both specialized and general skills in computer crime prosecutions. Specialized skills come from the High Tech Crime Team while general skills have been developed through training and handling cases.

Baltimore County, Maryland Police Department Economic/Computer Crime Unit

The Economic/Computer Crime Unit was established in March 1986 with the assignment of two investigators. The unit had been three years in the planning process, starting in July 1983 with a department committee formed to assess the impact of computer crime on the department and the community. As a result of the committee, a project team was established with the commanding officer of the Criminal Investigation Division serving as project manager. Creation of the unit was also encouraged by the Police Foundation, a local nonprofit support group in the county.[15]

The Computer Crime Unit is organizationally placed under the Fraud Unit of the department's Criminal Investigation Division. The two investigators were appointed to the unit after an extensive selection process. One investigator has been with the department for over 15 years and has specialized in the investigation of white-collar crimes, particularly embezzlements. This investigator had no computer background prior to this assignment. The other investigator, formerly with the Narcotics Unit of the department, had become personally interested in microcomputers as a hobby. He was selected because of the knowledge he had obtained on microcomputers. It was believed that this combination of investigative and technical skills was the ideal approach for the unit's activities.

The objectives of the unit are to:

- Establish and maintain lines of communication and cooperation with community groups to enhance the police effort to detect, investigate, and prevent computer crime.
- Monitor the existing laws and proposed legislation focusing on computer crime; and identify/recommend further legislative needs.
- Investigate computer crimes reported to the department.

The training received by these two investigators consisted of a three-month internship with the county's data processing section, approximately two weeks spent with the data processing section of the Baltimore Gas and Electric

Company, and the introductory course on computer crime investigations offered by FLETC. The time with the utility company was suggested by the Police Foundation and was particularly beneficial since it allowed for "hands-on" experience with data processing professionals. The company educated the investigators in how a large data processing facility operates and the security measures taken to protect the systems. It was later learned that the utility company also benefitted from taking a closer look at their security and from the probing questions of the investigators.

The FLETC course, called the "Computer Fraud and Data Processing Investigations Training Program," is taught by instructors with extensive field experience in computer crime investigations. Topics covered in the class include computer security, types of computer crimes, investigative techniques, and legal issues. Many case studies and exercises are given to provide practical experiences to the class members.

During the first year of operation, the unit members spent approximately 50 percent of their time on advertising their presence both internally to the department and externally to businesses. For officers in the department, a "training bulletin" was written describing the legal provisions of computer crimes in the state statutes and giving a procedure for officers to report computer crimes. Specifically, the bulletin states that any officer responding to a criminal incident where a computer is involved will submit a report to the unit for further investigation.

The two investigators in the unit have also given speeches at numerous school, business, and association functions. These speeches were aimed at explaining computer crimes to the audience and responding to questions on legal issues surrounding computer crimes. The talks at the schools have described the laws dealing with illegally copying programs and with hacking programs. At business and association functions, they have advised businesses on how to prevent computer crimes and urged them to report computer crimes when they occur. Through these talks, the existence of the unit has become known in Baltimore County and surrounding jurisdictions.

A related activity of one member of the unit is to respond to questions on a local bulletin board. This board is popular with high school students for exchanging games and messages. For example, one student asked whether the release of a new version of a popular software package meant that prior versions were in the public domain with the implication that they could be copied and distributed without restriction. The response from the detective was that such an activity would be illegal since it amounted to software piracy.

The unit coordinates its cases with one prosecutor in the State Attorney's Office of the county. This prosecutor, who has other responsibilities in the office, has worked with the unit since its inception and is now a specialist in computer crime laws. The standard operating procedure is to have the attorney involved in a

case from the start to assist with search warrants, arrests, and case disposition. At the time of this study, the unit had successfully adjudicated every arrest made through pleas, and no case had advanced to the trial stage.

Over a two-year period, the unit handled 41 computer cases including embezzlements, software piracies, bulletin boards, and Trojan horse offenses. Thirty-five persons have been arrested on these cases and charges placed against these individuals have always included computer crimes. *All* arrested persons have pled guilty but in many instances, the computer crime charges have been dropped or reduced as part of the plea negotiation process.

The effectiveness of this unit is also reflected in many additional duties they have been asked to perform. Several surrounding jurisdictions have requested their services to assist in computer crime cases. Generally they have been asked to check a microcomputer for information or to provide clarification on legal issues. They have also developed an investigative plan which gives general guidelines on how to approach the investigation of telecommunications crimes. The plan has been used as a training tool for other investigators. Finally, in conjunction with a telecommunications company and a telephone company, they developed a one-day training course on telecommunications fraud cases. Developed to create interest in these investigations by other police agencies, the course covers investigative techniques, demonstrations of electronic boxes and hacking programs, and prevention tips for businesses.

Illinois State Police
Computer Crime Section

The Computer Crime Section of the Illinois State Police was formally established in 1986 with two investigators. The management of the state police believed that computer crime was a growing problem in the state and that they should start taking steps to address the problem. Their approach was to create the Computer Crime Section and provide as much training as possible to the investigators selected for the section. Further aims were to solicit cases in order to obtain investigative experience and to establish contacts with private industry to work on the prevention of computer crimes.

From a slow start of only one true computer crime case during their first year of operation, they are now involved in approximately 25 new cases each year. Types of cases handled by this unit include credit card and phone card frauds through telecommunications, hacking, Automatic Teller Machine (ATM) and check frauds, illegal bulletin boards (including pedophile, cult, and sexually-oriented boards), and other telecommunications crimes.

These cases are handled in different ways, depending on whether they have been reported directly from the victims or from other agencies. All cases within their mandate that have been directly received from victims will be completely handled within the section. A case from another agency in the state is handled

in different ways based on the capabilities of the particular agency. Section investigators may assist the other agency on a limited basis; the decision may be made to work the case jointly; or the section may take over the case entirely for investigation.

As with Baltimore County, the FLETC training course has been the only formal classroom training received by these investigators. However, they have had extensive contact with long-distance carriers and other telecommunications companies because of the nature of their investigations.

Of particular note with this unit is that most of the cases are complicated since they involve telecommunications across jurisdictions and sometimes into other states. A case may be investigated for weeks before sufficient information is obtained for an arrest. A telecommunications case may require cooperation with a local telephone company, several long-distance carriers, and other law enforcement agencies.

The unit members also give numerous speeches throughout the state to organizations interested in computer crimes. These have included security associations, banks, long-distance companies, internal auditors, schools, microcomputer associations, and insurance companies. These talks have been particularly beneficial in explaining the state laws to these audiences and establishing relationships that have subsequently helped in investigations.

Los Angeles, California Police Department Computer Crime Unit

In the Los Angeles Police Department, interest in computer crimes as a special emphasis began in 1974 with a department order that assigned responsibility for computer crime investigations to the Major Frauds Unit of the Bunco/Forgery Division. Over the next ten years, computer crime cases (generally only one or two cases each year) were assigned to one or two detectives who had received special training in these investigations. These cases were part of the general caseload of these detectives and were regarded as interesting novelties of white-collar crime.

The Computer Crime Unit was established in March 1985 with the reassignment of two detectives from the Division. By that time, computer crime cases had become increasingly more complex than cases previously investigated. Further, reports of computer crimes had increased to the extent that it was no longer feasible to absorb them into the general caseloads of detectives in the section-a problem further complicated by the retirements of the two detectives who had received advanced training in computer crime investigations.

The major responsibilities of the unit are as follows:

- Investigate all crimes in the city in which computers are the object of attack.
- Investigate all crimes in which computers are the vehicle for the commission of criminal acts.
- Investigate all telecommunications crimes and thefts of telecommunications services.
- Provide training for department personnel in computer and telecommunications subjects.
- Provide technical assistance to other department and city units in support of their investigations.
- Develop public, private sector, and law enforcement agency relations in areas associated with crimes involving computers.
- Respond to requests for public appearances and speaking requests on areas such as computer crimes, computer and data security, and computer ethics.

The senior member of the unit has been on the department for over 20 years with 15 years devoted to investigations of white-collar crime. This investigator was assigned his first computer crime case in 1981 and has been specializing in this area since that time. In 1985, the second detective was assigned to the unit. Both have received outside training in computer crime investigations. In fact, the senior investigator now is a trainer for the FLETC courses.

The number of cases reported to the unit has steadily increased from 9 cases in 1985 to 17 cases in 1988. A total of 50 cases have been reported over these four years broken down by type of case as follows:

- Sabotage (9)
- Malicious access (8)
- Theft of services (7)
- Hackers and phreakers (6)
- Telecommunications fraud (6)
- Theft of information (5)
- Data diddling (4)
- Logic bomb (2)
- Mail fraud (1)
- Software theft (1)
- Software virus (1)

Of these 50 cases, 5 cases were referred to other agencies and 38 cases have received investigative attention by the unit. The unit has made 17 arrests, resulting in 15 convictions. Seven of the cases are still open.

Because of the size of the city (3.5 million persons and 433 square miles), the unit has to be very selective on the types of cases handled. As a general rule, they investigate cases in which the offense either has some degree of technical skill or involves the computer's operating system. Other cases, such as thefts of hardware and cases involving low monetary losses, are handled by other detec-

tives in the Major Frauds Unit or by district detectives. Cases investigated by the Computer Crime Unit generally require an extensive amount of investigative time to obtain the information and develop the evidence needed for successful arrests and prosecutions. The workload of the unit has increased significantly in recent years, and as discussed at the end of this chapter, more investigators are probably warranted for the unit to ensure that sufficient investigative time can be devoted to their cases.

The unit has also been active in working with the business community of the city on preventing computer crimes. The senior investigator is President of the High Tech Crime Investigators Association which establishes liaison with the business community on the subject of computer crimes. He is also a member of the association's board of directors. The Association, which is a membership fee organization, is an outgrowth of DATTA, described earlier.

Another interesting coordination activity in the Los Angeles area is the Computer Crime Task Force under the Countywide Criminal Justice Coordination Committee. Task Force members include representatives from surrounding law enforcement agencies, county data processing departments, and businesses. One of their activities has been the preparation of a pamphlet that gives tips on how businesses can reduce their vulnerability to computer crime as well as agencies to call when a computer crime is detected.

Maricopa County, Arizona Sheriff's Office Technical Crimes Investigation Unit

The background of this unit started with the interest of two investigators in microcomputers and telecommunications. In 1984, they established a bulletin board, called the Maricopa County Sheriff's Office Public Access Bulletin Board (PABB), on a microcomputer in the department for the purpose of increasing the awareness in the computer community of the services of the Sheriff's Office. Because bulletin boards were becoming popular at that time, the department felt that the PABB would advertise to the public that the Sheriff's Office was also interested in high technology applications.

The PABB led to one of the first computer crime cases handled by these two investigators. A user of the board left a message about another bulletin board called the Phun House, which was disseminating access codes to a local company that offered information network services. The message also gave instructions on how to access this board, including the password to the system. A subsequent investigation showed that access codes were, in fact, available on the Phun House and that the company was a victim of fraud on their system. The operator of the bulletin board was then arrested and charged with facilitation of computer fraud. From the information obtained in this case, three other computer crime cases evolved which also led to arrests and convictions.

Based on these successes, the two investigators received permission to establish a bulletin board to operate as a Sting operation for determining other computer crime activities in the Phoenix area. Approval was obtained and the bulletin board began operation in mid-1985. This bulletin board operated for approximately 12 months and resulted in over 50 arrests of individuals, most charged with telecommunications fraud.

This Sting operation with a bulletin board was the first of its type in the country. Since that time, other law enforcement agencies have used the technique. There are two primary advantages of a Sting operation. First, it is a convenient way of identifying hackers in the area who are illegally accessing other systems; most Sting operations have resulted in a high number of arrests. Secondly, such an operation may deter youthful offenders from continuing to commit computer crimes. Most of those arrested are juveniles and they generally receive light sentences. However, the arrests and exposure to law enforcement may cause these juveniles to cease their illegal activities. (Sting operations are discussed in more detail in Appendix A of this report.)

The Technical Crimes Investigation Unit was established in 1985 as a natural extension of the Sting operation and is organizationally part of the Major Felony Section. Current staffing remains at two investigators who handle computer and telecommunications crimes for the entire county. One of the two original investigators is still with the unit, and the other investigator has been with the unit for over two years. Their caseload is usually between 10 and 15 new cases each year.

The senior investigator of the current team has an extensive background in electrical engineering and radio operations. He has been with the department for 11 years and has received outside training on computer crimes through the IACP and FBI courses. Like the other computer crime units, public presentations is an important part of his job. The senior investigator has discussed computer crime with associations of accountants, state and local government computer users, and local clubs.

As a final note, the PABB continues to operate. Citizens use the board to send messages to any county agency. In addition, some users have exchanged files through the downloading capabilities of the system, and police departments in the area leave messages for each other through the board. Like Baltimore County's experience, the unit also responds to questions through the bulletin board. Finally, of particular benefit to the unit is that cases have been developed from confidential mail received on the PABB describing illegal information on other boards (pirate boards).

Santa Clara County, California Units

The San Jose and the Santa Clara Police Departments each have two investigators for computer crimes. In San Jose, one sergeant and one officer comprise

the High Technology Detail of the Fraud Unit while in the city of Santa Clara, two sergeants assigned to the Fraud Unit focus on the investigation of computer crimes.

Since Santa Clara County is the heart of "Silicon Valley" with its high concentration of computer companies, these units handle a variety of computer crime cases. Their cases have included telecommunications crimes, thefts of hardware and software, thefts of precious metals (used in manufacturing computer hardware), bulletin boards, and internal computer crimes. Over the 1988 fiscal year, the San Jose unit was assigned 45 new cases. This caseload is much higher than other units participating in this study and is particularly noteworthy because of the complexities of many of the cases.

Private investigators are also hired by many businesses in the county to investigate computer crimes inside the organizations. These investigators frequently coordinate their activities with the two police departments, and in some instances, will turn the case over to the appropriate department for further investigation, arrest, and prosecution.

The fact that businesses hire private investigators illustrates two points. First, many businesses are reluctant to report computer crimes to local law enforcement agencies and often conduct their own investigations. While arrests and prosecutions may result from these investigations, dismissal of an employee is frequently the result, and the law enforcement agency may never hear about the offense. Secondly, the police departments would not be able to handle all the computer crimes if they were reported. As a result, the departments sometimes suggest the use of a private investigator when the case appears to be particularly time consuming.

In the Santa Clara District Attorney's Office, one attorney has been assigned to handle computer crime cases. He assists all the law enforcement agencies in the county with their computer crime cases. He is known as being particularly aggressive in taking cases to court and has an outstanding record of successful prosecutions. He handles about 40 computer crime cases a year.

All these units are an outgrowth of DATTA, which is described in detail in the next section of this report. One of the objectives of DATTA was to provide training through seminars on computer crime topics to investigators and prosecutors in the county. It was the only outside training received by the personnel in these units.

Tarrant County, Texas Office of the Criminal District Attorney Economic Crimes Section

The Economic Crimes Section of the Tarrant County Criminal District Attorney's Office is responsible for prosecuting all white-collar crime in the county, including all computer crimes. The unit, which has been in existence since 1980, currently has a professional staff of two attorneys (one is the section

chief), two investigators, and a financial analyst (an accountant). This group will perform their own investigations and also assist local police departments and the sheriff's department in investigations.

None of the members of the unit has received outside training. However, the section chief has taken courses in data processing at a local university and has a personal computer system at home where he has written several computer programs.

The unit has had an emphasis on computer crimes since 1985 and currently investigates 10 to 15 cases each year, including telecommunications crimes, illegal bulletin boards, internal computer crimes, thefts of software, and thefts of trade secrets.

Members of the unit have also spoken at local colleges on white-collar crimes and computer crimes, and the section chief has given speeches in California to high-technology crime associations.

District Attorney's Technology Theft Association (DATTA)

In September 1984, the California legislature passed a bill to provide funding for a two-year pilot District Attorney's Technology Theft Association (DATTA) project for the prevention of high-technology crime. Santa Clara County was designated as the project location because it contains "Silicon Valley," the largest concentration of high-technology industries in the state. The county government and law enforcement agencies had been attempting to resolve the lack of coordination and communication between industry and law enforcement involving high-technology crimes. The business community was also looking for solutions and had created the Industrial Security Managers Group (ISMG) comprised of senior management and security personnel from 34 major computer manufacturers in the area. The pilot project offered an opportunity for these groups to coordinate and focus on prevention of high-technology crimes.

As used in the legislation, "high technology" was defined as "any technology requiring the most sophisticated techniques such as microelectronics, data processing, genetic engineering, and telecommunications." From a practical viewpoint, computer crime was the focus of the project with emphasis on internal computer crimes, software piracies, illegal access of systems, hardware thefts, and trade secrets.

The County's Office of Criminal Justice Planning (OCJP) was authorized to administer the project funds and to supervise the implementation of project activities. The project had four major structural components:

- An appointed nine-member Advisory Board.
- Three full-time project staff from the District Attorney's Office headed by a Deputy District Attorney.
- The Industrial Security Managers Group.

- A law enforcement association comprised of 28 detectives from local jurisdictions, 12 investigators from state and federal agencies, and 35 representatives from law enforcement agencies outside the county.

The Advisory Board, which provided overall guidance for the project, was comprised of representatives from the Santa Clara County District Attorney's Office, Santa Clara County Sheriff's Office, California Department of Justice, three high-technology industries, and three law enforcement agencies (Police Chiefs).

In an effort to provide as much support as possible to the participants, DATTA established several broad objectives:

- To increase awareness and commitment of time spent by participating agency personnel in the area of high-technology theft investigations.
- To create a central intelligence clearinghouse for information on high-technology crimes.
- To train unit participants in the area of high-technology theft investigations.
- To increase and enhance the communication links between police investigators, the district attorney's office, industrial security managers, and federal and state law enforcement agencies.
- To establish an organizational base for the development of a regional high-technology theft prevention effort.
- To conduct a statewide needs assessment for the development of a high-technology theft prevention effort in other California counties.
- To effectively prosecute high-technology cases in Santa Clara County and to assist in the creation of an effective prosecutorial foundation.

Over the two-year period of its existence, DATTA performed many activities and achieved several noteworthy results:

- Twenty-two of the law enforcement agencies in the county assigned detectives to high-technology crimes on either a part-time or full-time basis.
- These investigators collectively accomplished the following:
  - Investigated 200 high-tech crimes
  - Made 74 arrests leading to 54 adult convictions and 9 juvenile convictions
  - Recovered hardware and components valued at $2,881,000
  - Recovered trade secrets and software valued at $3,530,000.
- Established a bulletin board for high-technology investigators to provide detailed descriptions of stolen properties and information to aid in the recovery of the property. The system also provided on-line

tutorials, resource files, and legal memoranda relating to high-technology investigation and prosecution.

- Conducted five seminars with a total of over 300 attendees.
- Established a fourteen-member committee for a crime prevention program.

Two problems were encountered during the pilot project. First, many agencies could not justify assigning full-time investigators to computer crime investigations because of the low volume reported to their agencies. There was little or no participation in DATTA from these agencies. Second, violent crimes and drug cases were increasing in many of these areas, and many departments felt they had to devote more resources to these problems rather than invest in high-technology investigations.

At the end of the project, another bill was introduced in the state legislature to expand the project to five other counties. For a variety of reasons, including the two problems just mentioned, the bill was not passed, and in March 1988, the organization officially no longer existed.

Since that time, an informal DATTA group has emerged. Still centered in Santa Clara County, the group is comprised of the Santa Clara County Sheriff's Department, San Jose Police Department, Santa Clara Police Department, Sunnyvale Police Department, and the Santa Clara County District Attorney's Office. It is directed by a steering committee comprised of two persons from each agency. DATTA also continues to interact closely with the ISMG in prevention activities.

The DATTA steering committee has also decided to be more focused on the types of crimes emphasized by the organization. Two specific provisions in the state statutes were selected for emphasis:

- Section 499C: Trade secrets, thefts, solicitation or bribery to acquire.
- Section 502: Computer system or network; intentional access to defraud or extort or to obtain money, property, or fraudulent intent, representations or promises; malicious access, alteration, deletion, damage, or disruption.

This does not mean that other types of high-technology crimes will be ignored. The plan is for other investigative units in the participating departments to become more involved in computer crimes. For example, the burglary unit would be assigned to all hardware thefts (precious metals, microchips, and systems). If assistance is needed in the investigation, a high-technology investigator would be available.

The high-technology unit of the District Attorney's Office has also assigned an Assistant District Attorney on a part-time basis to prosecute hardware thefts. This will enable the Deputy District Attorney to concentrate on the more time-consuming access and trade secret cases.

Training continues to be a major concern of the DATTA group. While formal training is not offered, the steering committee has planned several activities:

- A series of video tapes to familiarize investigators with computer terminology and investigative procedures.
- New investigators assigned to computer crime units will be sent to training in each of the participating DATTA departments. This training will enable investigators to gain expertise by working with skilled investigators.
- DATTA will use guest speakers with expertise in high-technology crimes. This aspect of training will be heavily supported by the ISMG.

DATTA has provided the agencies in Silicon Valley with a unique organization to deal with computer crime. It gives prosecutors, law enforcement, and the business community an excellent forum to interact. In summary, DATTA has accomplished the following:

- DATTA has enabled agencies to gain knowledge and insight into the causes and scope of high-technology crime. It has assisted agencies in properly categorizing computer crime and collecting relevant statistics.
- DATTA has enabled law enforcement and prosecutors to focus their efforts on computer crime. It also allows them to key industrial targets of these crimes.
- DATTA allows law enforcement and the computer industry to interact and define common problems. This cooperation has strengthened both groups' resolve to report and solve computer crimes.
- High-technology crime is a problem that requires special attention and action. The level of effort, preparation, and information required to prosecute high-technology crime cases is complex and constantly changing. DATTA provides a means to educate and open communication between prosecutors, police, and industry. This interaction has allowed them to successfully prosecute criminals.
- Because of the technical aspect of most high-technology crimes, special training is needed for detectives assigned to computer crime units. DATTA has helped to define the type of training needed and in many instances has been the provider of the training.
- Education of the business community in crime prevention techniques is a top priority of the law enforcement community. Through DATTA the law enforcement community has been able to work very closely with the high-technology computer business community.

Organizational Experiences with Dedicated Units

Advantages and Disadvantages of Dedicated Units

The experiences of the agencies participating in this study offer several lessons on the advantages and disadvantages of establishing special units for investigating computer crimes. The primary advantages are (1) availability of a trained resource for computer crimes, (2) improved public relations with the business community, and (3) availability of personnel to assist in the development of computer systems for the agency. Each of these is discussed in the following subsections.

Availability of a trained resource for computer crimes

As discussed in Chapter 1, computer crimes are increasing each year in all parts of the country, and almost all states now have statutes on computer crimes. Because of their unique characteristics, these crimes offer an especially difficult challenge for local law enforcement and prosecutor agencies which historically have not had to deal with technically sophisticated crimes.

Having a special unit for computer crimes is one way of developing in-house talents to address these offenses. Many computer crimes are complex, requiring technical knowledge of computer hardware, software, operating systems, database packages, and telecommunications. Investigators must be able to converse easily with systems analysts and programmers to obtain information and identify offenders. These skills can only be acquired through training and practical experience derived from investigating cases.

A byproduct of having a special unit is that the personnel are available to assist in other investigations. The High Tech Crime Team in the Alameda County District Attorney's Office exemplifies this approach with members of its team available to assist all prosecutors in the office. In police departments, investigations of narcotics and other cases are starting to involve computers. The computer crime unit can assist with these cases when needed.

Improved public relations with the business community

As indicated by the responsibilities of the units in this study, working with the business community is an important activity of the personnel in a special unit. One chief of police stated that one of the reasons for establishing a special unit was to respond to concerns by businesses about computer crimes. A special unit lets the businesses know that local government is concerned about these offenses and is available for investigations. Relations with the business community can be further enhanced if an organization such as DATTA can be established in the jurisdiction.

In addition, the prevention aspects of computer crime cannot be overlooked. Businesses need information on how to protect themselves from being victims

of computer crimes. Personnel in special units are in an ideal position to provide (1) technical guidelines on how to protect hardware and software, and (2) operational guidelines to improve procedures, such as personnel screening or not giving any employee full authority on file changes.

Availability of personnel to assist in the development of computer systems for the agency

Agencies frequently need assistance in the development and implementation of computer systems for internal applications – particularly with the proliferation of microcomputers in most agencies. Data processing personnel are frequently not available to assist because of heavy demands to develop and maintain other systems.

A byproduct of a special unit is that in-house personnel become knowledgeable about how to design and implement computer systems. This is particularly true with spreadsheet and database systems for microcomputers. An investigator from the computer crime unit can assist another unit in setting up an application. This approach can be particularly cost effective and result in improvements throughout the department.

While the advantages of creating computer crime investigation units are numerous, there are also several disadvantages. These include the commitment of personnel to a white-collar crime, relatively low caseloads compared to other investigative units, continued need for outside resources for investigations, and the loss of unit personnel for other jobs. Each of these disadvantages is discussed in the following sections.

Commitment of personnel to a white-collar crime

The overwhelming problem in many jurisdictions today is drugs, not white-collar crimes. Police chiefs and prosecutors are under considerable pressure to devote any available resources to narcotic enforcement. It is therefore difficult for them to establish new units for any purpose.

Low caseloads

Compared to other investigative units, the computer crime units have relatively low caseloads. However, a comparison based solely on the volume of cases is unfair since the complexities of computer crime cases are not taken into account. As explained in Chapter 3, computer crime cases, particularly telecommunications crimes, require an extensive amount of investigative time. They frequently involve several long-distance companies, common carriers, and local telephone companies; and they may cross into other jurisdictions and other states. Obtaining cooperation from these groups and coordinating an investigation is sometimes an arduous task. Because of the nature of their cases, these units will always have numerically smaller workloads than other investigative units.

Outside resources for investigations will still be needed

Even if a special unit is established, experts from outside the agency will still be required for some cases. It is impossible for anyone to be completely knowledgeable about all the computer hardware, software, and operating systems available on the market today. Most investigators become acquainted with "DOS-based" systems since these are the most popular. When they come across other types of systems, they need to be able to call on someone for assistance.

Outside groups to consider for help include hardware and software vendors, computer clubs, users groups, universities, and individual consultants. Specialized associations, such as the Institute of Internal Auditors, American Institute for Certified Public Accountants, and EDP Auditors Association, may also be useful in an investigation.

Unit personnel may leave for other jobs

The expertise obtained by these investigators is valuable to many businesses. In particular, large companies sometimes have their own internal security and investigative units for data processing. The training and experience of the investigators in the computer crime units is ideal for these positions. A local agency should expect that some personnel will eventually leave for these positions.

In summary, the agencies in this study believe that the advantages of establishing a special computer crimes unit outweigh the disadvantages. Some of the units have been in existence for over ten years and have proven their value. Others with less time are well accepted, and there are no indications that the management has any regrets about establishing them.

In fact, the challenge in virtually all the units is how to control their increasing workloads. Guidelines limiting the scope of the cases handled sometimes have to be developed in order to concentrate on the most serious cases. In addition, the commanders of these units listed additional activities, such as Sting bulletin boards and more prevention activities, which they would like to perform if they had the personnel.

Responsibilities of a Computer Crime Unit

Before presenting the requirements for a computer crime unit, the responsibilities of such a unit should be discussed. Computer crime units usually have the following major responsibilities:

- Investigate computer crimes and/or prosecute computer crime offenders.
- Actively participate in efforts with the business community to prevent computer crimes and encourage the reporting of all computer crimes to law enforcement agencies.

- Interact with schools, computer clubs, and related associations to increase their awareness of computer crimes.
- Recommend changes, as needed, to strengthen computer crime legislation.
- Maintain up-to-date knowledge on computer technology, including computer hardware, software, and operating systems.

This list emphasizes that the responsibilities extend beyond the investigation and prosecution of computer crimes into duties not ordinarily found in investigative units. For example, establishing relationships with schools, businesses, and associations is an important activity. These relationships have proven beneficial in preventing computer crimes, in increasing the reporting levels of these crimes, and in identifying outside resources to assist in investigations.

Computer technology changes rapidly and new misuses follow the changes. A lag then develops between the language of criminal statutes and the misuses. Definitions must be added to the statutes, new computer crimes must be defined, and provisions for sanctions must be stated. The prosecutors in the units studied have been particularly active and effective in improving statutes in their states.

Finally, all the personnel in these units stated that they had a challenge in maintaining their knowledge and skill levels on computer technology. Because of the rapidly changing nature of computer technology, the continuing education of investigators is important enough to be stated as a specific responsibility. Investigators and prosecutors must devote a portion of their time to computer trade journals and other technical publications. They should also attend computer trade shows and outside training classes on the latest developments in computer technology.

Requirements for a Computer Crime Unit

Based on the histories of the units in this study, the steps required to establish and maintain a computer crime unit are the following:

- Select personnel.
- Provide training.
- Obtain hardware and software.
- Develop coordination between police and prosecutors.
- Establish relationships with the business community.

Each of these steps is discussed below.

Select Personnel

Computer crime units need personnel who are experienced in investigations of white-collar crime and who understand computer technology. Since both skills are rarely found in a single investigator, the computer crime units have generally been comprised of personnel with expertise in one area or the other. The Economic/Computer Crime Unit in Baltimore County is a good example of how two investigators have combined into an excellent team for computer crime investigations. One investigator has over ten years as a white-collar crime investigator but no computer experience and little interest in learning about computers. The other investigator, with a personal interest in microcomputers, has acquired an excellent technical knowledge of hardware and software. This is his first assignment in the detective bureau. In combination, these two investigators have solved several difficult embezzlement, telecommunications, and software piracy cases.

Personnel selection criteria also needs to include an ability for public speaking. Personnel in these units must interact with school and business organizations. Public speaking is, therefore, a key part of the job. Some audiences will be unfamiliar with computer crimes so that the investigator must be able to explain the statutes in simple terms. Other audiences, such as computer clubs, may be well versed in computer technology, and the investigator must be able to respond to their technical questions on their level.

The number of personnel needed in a computer crime unit is more difficult to address. None of the units in this study has more than four investigators and most have only two investigators. For areas such as Los Angeles, California and Maricopa County, Arizona, with their high population densities and technology centers, two investigators have proven inadequate for the caseload. These units screen the types of cases they investigate and do not have sufficient time for proactive operations, such as Sting operations, and for more prevention activities. All the units expressed the need for more personnel and supported their claims by noting that they did not investigate all types of computer crimes and were not doing enough preventive activities. Instead, the units tend to specialize in the computer crimes that match the skills of the investigators.

Discussions with the commanders of the units in this study suggest that five investigators can be justified. Two investigators with skills in computer technology are needed along with three investigators with good investigative backgrounds. The most frequent types of cases for these investigators will be embezzlements and telecommunications cases, including hacking and illegal bulletin boards. These cases can be split among the investigators to take advantage of their special skills.

Provide Training

When a computer crime unit is established, the training needs are extensive and immediate. Training must be provided on all aspects of computer technology. One training expert on computer crimes has suggested that two levels of training are needed: general investigative training and technical expert training.

The general investigative training can be covered in a three to four-day course on the following topics:

- State statutes
- Investigative techniques
- Search warrants
- Handling computer evidence
- Computer literacy

The logic behind this approach is based on cases that have been successfully handled in the past. A discussion of state statutes is, of course, needed so that the investigators understand what constitutes a computer crime. Search warrants are particularly important since most cases will result in a warrant to obtain further information or seize a computer system and related devices. The handling of computer evidence is becoming more important as defense lawyers learn more about how to defend their clients. Finally, all investigators need to attain a minimum level of computer literacy. It cannot be expected that this can be achieved in a short course. However, there are several useful books available and on-the-job training will eventually result in increasing the level of knowledge about computers.

Training someone to be a "technical expert" is a more difficult task, and an introductory course along these lines needs to be two to three weeks in duration. Topics covered should include the following:

- Computer hardware (from microcomputers to mainframes)
- Operating systems
- Application software
- Telecommunications and illegal telephone devices
- Bulletin boards
- Audit trails
- Security techniques

The need to acquire knowledge about computer hardware, operating systems, and other software is obvious. In a course of a few weeks, it is not possible to

cover these topics in the necessary depth, and investigators will continually be adding to their technical knowledge.

Telecommunications is an important technical area for investigators. In addition to learning about numerous illegal electronic devices, investigators need to understand the current organizational operations of common carriers and local telephone companies. Information on network services, such as CompuServe and The Source, also needs to be presented and demonstrated so that the investigators understand how these services operate.

Bulletin boards are also a special topic for investigators. Most of the units in law enforcement agencies have become well acquainted with bulletin boards. Many have investigated boards with illegal information on them, and in the case of the Baltimore County and Maricopa County units, bulletin boards are used in response to questions.

Audit trails and security techniques are two final technical topics needed by investigators. Audit trails are important because many of the cases involve embezzlements within financial institutions. Security techniques are expected to become more important in the future as offenders develop procedures to protect their systems. Passwords and encryption techniques are more likely to be used in the future.

Unfortunately, there are few alternatives from which to select for these training courses.[16] As discussed earlier in this chapter, the course offered at FLETC is one of the most popular for computer crime investigations. Most of the investigators have been to this course, and some now participate in the training. The course is particularly good since it emphasizes actual cases.

An alternative for general information can be found in the courses offered by local colleges and universities. Courses on microcomputers are usually available as well as advanced courses on computer hardware and software. If these courses are available, the law enforcement agencies and prosecutor offices need to bear the financial burden for them.

A final alternative for training, discussed in the section on Baltimore County, is for investigators to spend time with the data processing sections of other governmental agencies and private companies. Many utility companies, for example, have developed good security mechanisms to protect themselves against disruption of services. Businesses have the same approach and have established security sections in their data processing divisions for this purpose. Investigators can learn a considerable amount from these units on how security procedures operate.

Obtain hardware and software

There are two reasons for acquiring computer hardware and software. First, unit personnel will be called upon to check systems, obtained through search

warrants, to determine the contents and potential value in a case. Secondly, unit personnel need to understand how bulletin boards and information network systems (such as CompuServe) operate in order to have better insight into misuses of these systems. These aims can only be achieved by acquiring hardware and software for internal use by the units.

The hardware and software needs can be almost completely satisfied with microcomputer systems. Most of the units in this study had microcomputer systems in their offices. In some instances, these systems had been purchased by the agency for general data processing applications and the unit personnel used the equipment for their purposes. In other instances, microcomputer systems had been obtained by court order from cases handled by the unit.

The primary manufacturers of the microcomputer hardware found in these units are IBM, Apple, Radio Shack, and Commodore. The unit in Baltimore County has several systems, and these systems have proven very beneficial in their investigations. The technical manuals for the systems have also been obtained, enabling the investigators to learn how the microcomputers operate and how to check the systems for possible evidence in a case.

Software needs fall into two categories: application software and "investigative" software. Application software includes many of the popular word processing, spreadsheet, and database management packages. When a system is found with one of the packages on it, the investigator needs to know how to operate the application in order to view the files and determine their value in a case.

Investigative software are programs that allow a detailed analysis of the system, particularly the hard disk. Examples of this software are Norton's Utilities, PC Tools, Mace Utilities, Ultrazap (a public domain package), Disk Jockey, and Locksmith. These software packages are intended for general use by microcomputer owners when they encounter problems with their systems. Their application as an investigative tool has been recognized by computer crime investigators.

One of the best uses of these investigative tools is to unerase files and to identify "hidden" files. In most microcomputer systems, erasing a file really means that the status of the file has been changed in the disk directory, but the data remains intact until some other program writes over the physical area. Provided that the data has not been physically destroyed, investigative software can change the file status in the directory, enabling the file to be retrieved and viewed. Another deception by some programmers is to change the status of a file to "hidden," meaning that the file still exists and cannot be erased, but the file name does not appear on any directory listing of the disk. Investigative software can find the names of these hidden files and list them for retrieval and review.

Develop coordination between police and prosecutors

Good cooperation between police and prosecutors is essential for the success of a computer crime unit. Many of these units are housed in police agencies, and in these instances, the prosecutors have designated an attorney to specialize in these cases. This arrangement has worked particularly well in Baltimore County, Maryland; Los Angeles, California; Maricopa County, Arizona; and Santa Clara County, California.

The process in these units is that the investigator and the prosecutor meet early in the development of the case. After reviewing the facts, the prosecutor can offer advice on how to proceed from a legal viewpoint for eventual arrest and prosecution. Details on what constitutes a computer crime, what evidence is necessary, how search warrants should be written, and what information from a system should be obtained must all be considered in these deliberations. Failure to address these questions as the initial step in a case can lead to the ultimate dismissal of the charges.

Another scenario for coordination is found in the Alameda County, California and Tarrant County, Texas prosecuting attorneys' offices. Both have prosecutors and investigators specializing in computer crime cases, and the coordination is facilitated since it is completely in-house. The local police departments contact them whenever a computer crime case arises. The coordination in these cases is exactly as described above with the prosecutor being introduced early into the case.

Two points should be made concerning prosecutors who specialize in computer crimes. The first is that these prosecutors have been instrumental in their states in improving the state statutes on computer crimes. The state legislature calls on these prosecutors for assistance in new legislation because of their specialized knowledge. Clarifications of computer terms and definitions of computer crimes have been added to the statutes as a result of their actions. Secondly, these prosecutors need to receive training along the same lines as the investigators in police agencies. Especially when first assigned, these prosecutors may have only a limited knowledge of computers and computer crimes. Training is needed to raise their knowledge level for handling these cases.

Establish relationships with the business community

A final important responsibility of all computer crime units is establishing relationships with the business community. Since computer crimes are underreported to law enforcement agencies, units must be proactive in urging business victims to report offenses. All too often the tendency of the business is to solve the problem internally and not report the problem to the police. An employee may be fired rather than arrested even when the financial loss to the business is large. Unfortunately, these individuals may subsequently be employed by other businesses and commit similar types of offenses.

Personnel in the units studied believe that *50 percent* of the unit's time in the first two years can productively be spent in developing relationships with the business community. In many jurisdictions, the local Chamber of Commerce may be a good starting point for initiating contact with businesses. Business members of the Chamber of Commerce usually are interested in working with local government, and there is sometimes a small business component as a special focus within the chamber. Regardless of how these relationships start, some of the main ways of obtaining support from business are by making presentations at meetings, working with individual businesses, and developing brochures to describe computer laws and the unit. These activities can provide prevention tips as well as encouraging businesses to report computer crimes when they occur.

Contacts with telecommunications and telephone companies also need to be developed by the computer crime units. Long-distance carriers (such as MCI and Sprint) and information service companies are located in many jurisdictions, and these companies are especially vulnerable to telecommunications crimes. The experience of the computer crime units is that these companies will report offenses to them if they believe that actions on arrests and prosecutions will be taken. Further, their cooperation is frequently needed to assist on-going investigations. By making personal contacts, the computer crime unit will be able to establish good relationships for investigations.

Chapter 3

Computer Crime Investigations

Cases Investigated by the Computer Crime Units

A review of the full-time units participating in this study shows that all of the units had conducted investigations of telecommunications crimes. Hacking and phone phreaking are the two most prevalent types of cases from this category. Many are reported by either the local telephone company or a long-distance carrier. These victims frequently know the telephone number of the offending party so that the investigators have an excellent starting point for the case.

Three of the units in this study – Maricopa County Sheriffs Office, Los Angeles Police Department, and the Illinois State Police – have caseloads almost exclusively in telecommunications crimes. Their cases include large frauds in which telecommunications play an important role. In addition, they have investigated many misuses of telephone systems. Interestingly, the investigative techniques are similar for most telecommunications and telephone crimes. Because of the high population density in these jurisdictions, it has not been difficult for these three units to develop full workloads on telecommunications and telephone crimes.

Other units have developed specialties based on the particular expertise of the investigators. Most of the caseload in the Baltimore County unit involves white-collar crimes and the unit has rarely had occasion to investigate other types of computer crimes. Other units in the study are located in the Silicon Valley area of California, and thefts of hardware and software have predominated in their caseloads. These thefts have frequently involved large amounts of hardware and potentially valuable trade secrets. In summary, the specializations of some of the units have evolved as a combination of the expertise of the investigators and the types of crimes peculiar to the geographic area.

In the following sections, eleven cases investigated by these units are presented to illustrate the investigative and prosecutorial skills needed for computer crimes and the results that can be obtained. Exhibit 3-1 provides a list of these cases along with the specific charges initially placed against the defendants. The computer crime charges (Chapter 4 presents the statutory definitions of these terms) include unauthorized access to a computer, harmful access to a computer, misuse of a computer service, disrupting a computer service, and possession of a device to avoid telephone charges. These cases also show that computers are involved in more serious offenses such as extortion, forgery, embezzlement, racketeering, prostitution, and grand theft.

Exhibit 3-1

Summary of Cases and Charges

Type of Case	Charges
Data Destruction and Logic Bomb Case	Burglary Harmful Access to a Computer Criminal Mischief
Hacker Case #1	Grand Theft Unauthorized Access to a Computer Theft of Services Theft of Credit Card Information Possession of a Device to Avoid Telephone Charges
Hacker Case #2	Unauthorized Access Theft of Credit Card Information Possession of a Device to Avoid Telephone Charges
Telephone System Seizure	Unauthorized Access to a Computer Theft of Services
Illegal Access Case	Illegal Access Fraudulent Use of Access Codes Disrupting Computer Services Misuse of a Computer Service Extortion
Embezzlement Case #1	Grand Theft Pursuant to a Common Scheme Forgery Fraudulent Misappropriation Unauthorized Access to a Computer
Embezzlement Case #2	Grand Theft Unauthorized Access to a Computer
Prostitution and Racketeering Case	Pimping Pandering Conspiracy
Software Piracy Case	Grand Theft
Theft of Silicon Wafers	Grand Theft
Theft of Trade Secrets	Grand Theft Unlawful Access to a Computer

The cases have been classified under the typology described in Chapter 1 to illustrate the specific characteristics of each category. The first case, *State of Texas* v. *Donald Gene Burleson,* involves the destruction of a large volume of computer records and the disruption of the company's services for several days. The defendant was found guilty of harmful access to a computer and was ordered to pay almost $11,800 in restitution to the company. The case was prosecuted by members of the Economic Crimes Unit in the Tarrant County Office of the Criminal District Attorney.

The location of the other cases in this chapter and the identities of the victimized companies have not been specified at the request of the participating units and the companies. As indicated in Chapter 1, many victimized companies want to avoid publicity about these offenses. The victims in this chapter include a popular telecommunications services company, a nationwide long-distance carrier, and a well-known software development firm. Their requests for anonymity have been honored in the descriptions.

In addition, the generic term "Computer Crime Unit" (CCU) is used in all cases to refer to the investigative unit from the local law enforcement or prosecutor agency. The chapter concludes with a discussion of the lessons learned from the cases handled by the units.

Internal Computer Crimes

Data Destruction and Logic Bomb Case

The victim company involved in this case is USPA & IRA, a licensed life insurance agency and registered securities dealership whose home office is in Fort Worth, Texas. Independent agents make sales for this company, and the agents are paid a commission based on their sales. At the time of the offense, commission payments averaged two million dollars a month to approximately 450 independent agents.

Most of the commissions are calculated from records on magnetic tapes submitted monthly by insurance and securities firms across the country. The company's mainframe computer processes these tapes and produces commission reports on a monthly basis. This computer process includes the creation of three commission "detail files" and a commission "master file."

It was discovered one morning that the computer system had suffered a major loss of records from the detail files. More specifically, over 160,000 records had been deleted from each of the three files, amounting to about 75 percent of each file. Without these records, the monthly commission report could not be created, and the independent agents could not be paid.

Through the history log on the system, the deletions were linked to system access which had occurred between 3:00 a.m. and 3:30 a.m. earlier that morning. Someone had used the system during this time period to run a series of programs

that resulted in the deletions of the records. Further investigation determined that these programs had been created approximately three weeks prior.

Three days before this incident, the company had involuntarily terminated Mr. Donald Gene Burleson, a senior systems analyst who had been with the company for two years. He was the Operations Manager and the company's computer security officer. After an initial investigation by the company, Mr. Burleson was determined to be the prime suspect. The company sued him in Civil Court for illegal trespass, breach of fiduciary duty, and gross negligence.[17] The jury agreed with the company's position and ordered the defendant to pay approximately $12,000 in damages.

Mr. Burleson was then charged in criminal court with burglary, harmful access to a computer with loss and damages over $2,500 (a felony offense in Texas), and criminal mischief over $750. After a two-week jury trial, he was found guilty. His sentence was seven years of supervised probation and he was ordered to pay $11,800 in restitution to the company.

The section chief of the Economic Crimes Unit was the prosecutor in this case. His extensive knowledge of computers and the state's computer law was very beneficial in the successful prosecution. While the defense attorney did not have a computer background, he was guided by his client throughout the case. In response to the criminal charges, the defense eventually filed 30 motions, including 13 discovery motions, three motions relating to challenges to the indictment, and three motions to dismiss related to destruction of evidence.

Like many internal computer crime cases, there were many complexities in this case. For example, anyone wanting to access the mainframe computer had to "sign on" from a terminal. The sign-on procedure required the person to first enter into the terminal an account name identifying the user. Then, a password uniquely associated with the account name had to be provided. Access was denied if someone attempted to use a valid password from another account name.

Mr. Burleson is believed to have committed his crimes in the following manner. On the day that he was terminated from the company, his account was removed from the computer system and a new password for the security officer was created. However, it is believed that he reentered the building three days later and accessed the computer using an account name he created prior to his termination. This account name was probably created for the specific purpose of allowing him access in the event he was terminated or quit. He then ran the security functions program that provided the security functions menu and the new security officer's password. With this information, he was able to bypass the security mechanism and obtain complete access to the system. A series of programs were then run which resulted in the destruction of the records in the three files.

As part of the automatic computer procedure, these programs were copied and given new names, and the old versions of the programs were deleted. Further, each destructive program read a data area to determine (1) the date that the deletion and copy programs should run next, and (2) the current names of the programs. This overall procedure would be activated by the programs creating the commission detail records and would result in the deletion of files on a monthly basis. It would also make the tracing of the deletions more difficult in the future. Fortunately, this procedure was found before it could be activated.

Other interesting features of this case are as follows:

- When it was discovered that there had been a major loss of records, the entire system was copied to 12 magnetic tapes. This step allowed analysis at a later date on exactly what was on the system at the time of the loss.
- One defense motion requested the use of the victim's computer to examine the backup tapes. Obviously, the company objected strongly to this request. While the motion was being considered, the state and the defense reached an agreement allowing the defense access to the tapes over one weekend on a computer system provided by the defendant. Further, the company controlled the loading of the tapes and the access to the information. All printed materials stayed in the possession of the state until released by agreement,or by court order.
- Appendix D shows the discovery motion filed by the defendant for system backup information. The motion illustrates the need for prosecutors and investigators to understand computer terminology. Among the terms used in the motion are "non-system save," "source code from all libraries on the NON-SYS," "copy of the Object dump," "copy of the Save Changed Objects," and "QHST logs."

Telecommunications Crimes

Hacker Case #1

An informant told the FBI about a bulletin board that contained credit card numbers, telephone card numbers, and other information. The FBI agent notified the CCU which arranged an interview with the informant at his apartment. During the interview, the bulletin board was accessed and information from it was printed. Since the bulletin board was located in another county, the CCU investigators did not have legal jurisdiction to continue the case. Unfortunately, the police agency in the other county did not have the expertise to investigate computer crime cases. As a result, the CCU told investigators from a long-distance carrier about the problem.

The long-distance carrier placed a Dial Number Recorder (DNR) on the telephone line of the bulletin board.[18] Results of the DNR showed frequent access into a telecommunications company's system located in the CCU's

county. This information allowed the CCU investigators to reenter the case since state law provides legal jurisdiction when the system being violated is within the county's boundaries.

A search warrant was obtained for the location of the bulletin board. Obtained during the search were three microcomputer systems, numerous diskettes, printouts, and several boxes of technical manuals. At the time of the search, one of the microcomputers was illegally accessing the system of the telecommunications company.

The hacker subsequently admitted to having established the bulletin board and keeping credit card and telephone account numbers on it. He was formally charged with grand theft, unauthorized access to a computer, theft of services, theft of credit card information, and possession of a device to avoid telephone charges. The final penalties in this case were restitution to the long-distance carrier, destruction of the computer equipment by court order, a $250 fine, 150 hours of community service, and three years probation.

Interesting notes about this case are:

- The investigators described this hacker as having a large ego – a common trait of hackers – which was fueled by the publicity surrounding the case. He accepted interviews from local newspapers and described his activities in detail. He also called the investigators on several occasions after the arrest to provide more details on his offenses and to brag about other capers.
- Printouts from other companies were found during the search. The hacker had obtained these printouts from local dumpsters. Checking dumpsters is a common practice of hackers.
- The hacker was a legitimate subscriber to several long-distance carriers and computer services. As a result, he had the usual customer documentation on access requirements and full use of services for legitimate purposes.
- The bulletin board contained other items including instructions on how to construct an explosive device. Ingredients for such a device were seized by the police from the apartment.
- The credit card and access numbers had been posted on his bulletin board for use by other hackers. Like many other bulletin boards, it had certain levels of access that could be obtained only after telephone contact with the hacker to prove "legitimacy."
- The statute on computer crimes in this state says specifically that the computer involved in an offense must be physically destroyed in the event that the owner is found guilty. By court order, the microcomputer belonging to this individual was therefore destroyed.

From the investigative viewpoint, one of the points made by this case is the need for investigators to coordinate their activities with telephone companies and long-distance carriers. It is frequently necessary for a DNR analysis to be performed in telecommunications cases in order to determine when and where calls are being placed. Another point in this case is that CCU investigators must sometimes coordinate their activities with investigators from other agencies who may not be familiar with computer crimes.

Hacker Case #2

The juvenile in this case was given a present of a microcomputer system costing less than $300. It included a keyboard, modem, and floppy disk drive. A television in his bedroom served as the monitor. The juvenile spent hours each week communicating with various bulletin boards. Initially, he contacted bulletin boards in his immediate geographic area to download computer games and other programs for his own entertainment. This activity eventually spread to bulletin boards across the country, including systems that contained illegal information. He spent enough time with these boards to become known as a regular and was provided higher levels of access into many systems.

From one of these bulletin boards, he obtained a "hacking" program. This program dialed the local access number of a telecommunications company and tried a randomly generated account number. If the number was not accepted, the program disconnected, dialed the access number again, and tried another account number. The program was activated in the morning before school and could try several hundred account numbers during the school day. As a result, there might be 20 valid numbers recorded on the system's diskette during this time. The hacking program operated automatically with no intervention needed on the part of the operator. A few of these numbers were used by the juvenile to call other hackers and friends around the country.

In addition, he established a bulletin board and posted several account numbers so that other hackers could obtain them. An unusual feature of the bulletin board was that it existed on a diskette since the system did not include a hard disk. During the four months of its existence, the bulletin board was accessed by more than 100 persons.

The individual was caught through the monitoring efforts of the telecommunications company. Telephone lines were periodically checked for unusual activity such as a large volume of calls to the same number in a short period of time. When the company detected this situation, it contacted the CCU which, in turn, obtained a search warrant for the home. During the search, the juvenile readily confessed to his actions.

His penalty from juvenile court was one weekend in juvenile detention, seizure of his computer hardware for several months, confiscation of all diskettes (not returned), and ten weekends of labor with other juveniles in cleaning parks and

other activities. His legal defense costs exceeded $1,400, which his family required him to pay from monies earned from odd jobs over three previous summers.

Other interesting notes about this case are:

- Six investigators, including representatives of the telecommunications company, went on the search of the house. This three-hour procedure had some "shock therapy" value on the juvenile and his family. The family had been completely unaware of his illegal activities.
- His arrest and subsequent sanction also had a deterrent effect on several of his friends who were performing similar operations. They immediately stopped their activities. In addition, the juvenile now cooperates with the police department in efforts to prevent others from committing these offenses.
- Like many hackers, this juvenile was an average student, but did not have many outside interests. The family believed that their son had found a legitimate outlet for his talents.
- The amount of loss suffered by the telecommunications companies cannot be determined on these types of cases since the account numbers posted on bulletin boards are changed frequently and can be obtained by hackers all over the country and even internationally.

Telephone System Seizure

This offense occurred within a medium-sized company that had purchased a computer-based telephone system for internal communications and long-distance calls. The system allowed employees to have the usual inter-office communications and included an accounting procedure for long-distance calls. Each person had his or her own internal identification number that was included on all long-distance calls.

A voice-mail capability was also part of the telephone system. Because the capacity of the voice mail exceeded the needs of the company, a decision was made to offer this service to outside subscribers as a sideline business. During the evening and weekend hours, this access was accomplished by dialing the company's main number, and the telephone system then switched the caller into the voice-mail system.

One of the subscribers, who was a student at a local university, accidently discovered a way to interrupt the switching procedure after dialing the company's number. The result was that he obtained an open telephone line, not requiring an internal identification number, that could then be used to dial whatever number he wanted. In essence, he could take over the telephone system and make long-distance calls with the costs billed to the company. This individual then charged other persons to make calls in this manner. Many of

the calls were placed to foreign countries (including Pakistan, India, and South American countries) and sometimes lasted over an hour.

The person in the victim company responsible for checking the monthly telephone bill quickly determined that there was a problem since the next month's bill showed approximately $6,000 in calls to countries where the company had no clients. However, the initial belief was that a mistake had been made on the bill as they had no reason to suspect that their system had been compromised. He immediately contacted the local telephone company and the long-distance carrier to have the invoice corrected. Checks were initiated by them to determine whether a billing mistake had occurred such as inadvertently placing another company's calls on the bill. Unfortunately, several months elapsed while these checks were being made.

In the meantime, calls to foreign countries continued to appear on the monthly billings, and the company continued to dispute the bills. After several months, the company finally contacted the police department for assistance. An investigator from the CCU was assigned to the case, and he immediately arranged for a trap and trace to be placed on the company's line. This procedure eventually identified the specific location of the telephone calls, and the student was arrested.

Charges placed against him were unauthorized access to a computer system and theft of services. After arrest, he refused to cooperate with his assigned public defender and two court-appointed attorneys, insisting that he could represent himself. Because of these problems, he spent several months in jail. The charges were eventually dropped based on the jail time, and the individual was released.

At the time of the arrest, the company had received bills for $108,000 for the calls plus another $40,000 in interest owed. The telephone company and long-distance carrier have always maintained that they were due the full amount for the calls since the internal system was compromised and their systems had nothing to do with the offenses. The company has maintained that the telephone company and long-distance carrier were slow to act and could have blocked calls to foreign countries after the first month. At the time of this report, there had been no resolution on the total bill, and the company has indicated that civil action may be necessary to resolve the dispute.

Illegal Access to Computer Services

As illustrated by this case, companies that provide computer services via telephone lines can also be victims of computer crimes. Located on the west coast, this computer service company provided several options to its customers including electronic mail, access to reference materials, bulletin boards, shopping capabilities, and automatic connections with other on-line services.

Access to the system was relatively easy since the company did not require the establishment of an account prior to the first use of the system. Instead, a person could dial into the system and provide name, address, and a major credit card number. All services of the system were then available to the person and charges would be made against the credit card for payment.

The adult involved in this case had a full-time job at a retail outlet where he stole credit card numbers from persons making purchases at the store. He shared the numbers and names with two juveniles through a bulletin board. The juveniles would then use the stolen credit cards along with the person's name and a fictitious address to access the system. Interestingly, one juvenile was located in a different state than the other two persons.

They also stole telephone card numbers from several long-distance carriers. In accessing the system, they would have one carrier dial another carrier and then dial into the system. With this "weaving technique," any attempt to trace the call starting from the computer system would only lead back to another carrier rather than the actual originating number.

These individuals, who had excellent computer skills, found ways to access parts of the system not usually available to customers. More specifically, they located the personnel information of the company contained in the system. Over a period of time, the company realized that parts of the system were being illegally accessed and they made software changes to block the illegal entry into their private files.

Unhappy about not being able to access all parts of the system, the perpetrators began to leave electronic mail messages addressed to top people in the organization. In these messages they threatened to destroy the databases and system programs if they were not provided unlimited access to all parts of the system. At this point the company contacted the CCU for assistance in the case.

Further investigation determined that the perpetrators were using several account numbers to access the system. The names and addresses of the accounts were checked by the investigators. While most had false addresses, one suspect was identified having an account with his correct name and address. Based on this information, a DNR was placed on the suspect's telephone lines, and the company through its computer system began to log all incoming calls from this line. During a thirty-day period, the suspect made 90 calls that compared exactly to 90 illegal accesses to the service.

On the basis of this information, the suspect was arrested. This person admitted to breaking into the system and implicated the other two persons. The CCU arrested the adult and juvenile residing in the state and contacted another law enforcement agency about the second juvenile (no further information is available on this individual). The adult and juvenile were charged with unauthorized access of a computer, fraudulent use of access codes, disrupting computer services, misuse of a computer service, and extortion.

While the extortion charges were eventually dropped, both the juvenile and the adult pled guilty to all four computer crime charges. The adult was sentenced to 90 days in jail and ordered to pay $5,000 in restitution to the victim company. The juvenile was sentenced to six months in the juvenile detention center and was ordered to give his microcomputer system to the company as partial restitution.

Computer Manipulation Crimes

Embezzlement Case #1

This embezzlement scheme, accomplished by an assistant manager assigned to the Accounts Receivable Section of a financial institution, centered around the standard practice of insuring loans against the death of the person receiving the loan. In the event of death, the institution could submit a claim to the insurance company for the outstanding loan balance. The only exception to this practice was that the company would not insure anyone over 70 years of age. The assistant manager was responsible for submitting claims to the insurance company.

The manager developed a scheme based on the loan line of credit available to a customer. For example, if the customer had applied originally for a line of credit of $10,000 and had an existing balance of $2,000 at the time of death, the $8,000 difference was subject to theft by the manager.

To perform the embezzlement, he would take advantage of the death of a loan recipient by generating a fraudulent loan for the available amount. Persons with authority to sign checks asked no questions because of the status of the assistant manager. The check was then deposited by the manager in an account with a fictitious name established by him for this purpose. Once the money was in this account, it could be transferred outside the institution for withdrawal. These steps kept everything except the final transfer within the institution, thereby averting an audit trail from another bank where the check would have cleared.

The manager then submitted a claim to the insurance company for both the original loan and the fraudulent loan. The claim was paid without question, and the financial institution was completely reimbursed for both loans. Neither the insurance company nor the estate questioned the loan since it had no effect on the estate value.

The scheme was uncovered through complications from a loan made to a person over 70 years of age. When the manager received notice of the death of this person, he followed his practice of generating a second loan and submitting a claim to the insurance company, not realizing that the person was uninsurable because of age. The insurance company rejected the claim. The manager's superior insisted on submitting the claim to the estate of the deceased, which subsequently paid in full. At this point, the fraudulent second loan was dis-

covered by the manager's superior, and the CCU was called to investigate. The manager confessed to the scheme after questioning by the detectives.

When arrested, charges against the manager included grand theft pursuant to a common scheme, forgery (two counts), unauthorized access to a computer, and fraudulent misappropriation. The unauthorized access charge covered the creation of the false accounts on the system and modification of other files reflecting the loans. His final sentence was five years of probation and restitution of $17,000.

Embezzlement cases usually have complicating details, as illustrated in this case by the following:

- The insurance checks were posted against an outstanding balance owed to the institution. They did not require endorsements since they were for deposit only to the institution. The institution had no reason to question either the posting or the loan balance since they appeared to have been generated in a normal manner.
- The checking accounts with fictitious names were established in a circuitous manner. The computer system allowed changes on all fields of an account *except* the social security number, which served as the account number and could only be changed by the Data Processing Section. The manager's scheme was to use his terminal to locate a valid account in the system. He would then write this name and a bogus social security number on a slip of paper and tell the Data Processing Section that the social security number on file was incorrect. They would change the number based on name verification thus creating a new account under a fictitious social security number. The manager would then change the name and other information on this account for his use. The final step was to tell the Data Processing Section that the original account had been accidently deleted and request the reestablishment of the account.
- Another problem faced by the manager was that the last bank statement for the deceased person listed the second loan. This loan was subject to question if the statement was received by the estate of the deceased. To avoid this situation, the manager would change the address of the account to a non-existent address. The statement would then be returned to the financial institution because of the bad address. The policy at the institution was to shred all returned statements. The manager would then go back into the system and correct the address. After six months, the deceased person's account was completely purged from the computer system. As a result, all computer evidence of the loan was destroyed.
- The manager destroyed all paperwork associated with the fraudulent loans and with the deposits. This paperwork was kept in a protected vault. However, the vault was left open during Board of Director's

meetings which often went past normal business hours. The manager would stay late to gain access. As a result, the only physical evidence in this case was a single deposit slip for the loan on which the manager was arrested. All paperwork on previous loans had been destroyed.

The investigation of this case proceeded in a normal manner for embezzlement cases. The investigators from the CCU interviewed persons at the financial institution to determine how loans were normally processed. With regard to the computer system, the primary questions involved were who had access to the system and who had authorization to make changes. The aim of the investigators was to find the weak spots in the loan process and the computer system subject to abuse by employees. The assistant manager was identified rather quickly as the primary suspect. When confronted with specific questions by the investigators, he admitted to the entire scheme.

As viewed by these investigators, most embezzlements are 90 percent detective work and only 10 percent computer work. That is, the basic approach to such an investigation has not changed because of computer technology. However, knowledge about computer systems is necessary to establish the details of the embezzlement process and to gather essential evidence for the case. At the same time, computer crime charges can now be brought along with the embezzlement charges.

Embezzlement Case #2

This embezzlement occurred within a personnel agency that specialized in providing registered nurses and nurses' aides on a part-time basis to medical facilities. The computer system which maintained time card information and generated paychecks was an integral part of the embezzlement scheme.

Two full-time employees were authorized to use the system. Each had a different password for access. One of these persons developed a scheme in which she created time card records and paychecks for a fictitious employee with a name close to her own. She also stole the password of the other employee so that all transactions for the fictitious employee appeared to have been done by her co-worker.

Daily batch files were created with the system reflecting who had worked at a medical facility for that day, the numbers of hours worked, and the hourly pay rate. These files were transmitted via modem to the company headquarters in Florida, which then transferred the necessary funds to the agency's bank for covering checks written These batch files were normally destroyed by the employee after the transmission. Personnel were paid by the local agency using pre-signed checks. It was common for employees to be paid on the same day they worked, and the paychecks were automatically printed by the system.

The scheme was to include the fictitious employee in a daily batch file showing hours worked for known clients of the agency. (In fact, she later stated that she created some batch files containing records for only the fictitious employee.) She then transmitted the batch file to Florida and created paychecks to the fictitious employee. Because the names were similar, she encountered no problems at check cashing establishments.

One of the mistakes of this individual was not to deduct social security from the checks made to the fictitious employee. In a routine accounting audit, the agency found a difference between social security owed based on the total payroll and the social security amount deducted from paychecks. The difference was traced to this employee because of her omissions from the checks. However, the police department was still not called into the case. Instead, the agency notified the check cashing establishment not to cash any more checks made out to the fictitious name.

The employee was arrested during an attempt to cash one of the checks. She was subsequently charged with grand theft and unauthorized access to a computer. Her actual sentence was restitution in the amount of $17,000, five years suspended sentence, six months at the County Detention Center, and three years of supervised probation.

Some of the interesting features of this case are:

- The individual would come to work during her off-duty hours to create many of the batch files. The company believed that she was a dedicated employee.
- The company performed no background checks on applicants. This individual had previous arrests and convictions.
- The company did not divide responsibilities between the two employees who operated the computer system. Each could establish accounts, enter time information, create paychecks, and delete files.
- The initial arrest by the patrol officer was for "Petty Theft of Checks." Fortunately, a report review officer recognized that a computer crime was involved and forwarded the report to the CCU for further investigation.

Support of Criminal Enterprises

Prostitution and Racketeering Case

The prostitution ring in this case had been operating in several cities and had revenues of at least three million dollars per year. Support for its operations had been computerized with three microcomputer computer systems. The primary system was comprised of five work stations connected to a 386-based file server for data storage. Another microcomputer was for the programmer,

who developed several sophisticated entry, update, and inquiry applications with a database management system. An accountant used the third microcomputer to maintain the financial records for the prostitution ring.

Located in a suite of offices in a business area, the systems were used in all aspects of the enterprise. There were 38 telephone lines into the offices. Prostitutes could call daily to provide the system with their availability. Requests from clients were entered by data entry personnel at the time of the call. Information on each client included name, credit card number, and preferences. A name search capability allowed the data entry personnel to run the client's name against the existing database. Comments placed in the system by the prostitutes could be retrieved in this manner. At the time of the arrests, there were more than 80,000 names in the database.

Prior to the arrests, the police department gathered extensive intelligence information on the activities of the prostitution ring and on the computer systems. They were able to determine the type of hardware, operating system, and programming language for the microcomputers. In addition, they were fairly certain that no hidden programs or hardware modifications existed that could erase files in the event of a raid.

Eighteen search warrants were issued based on the intelligence information. When the warrants were executed at the central location, several officers were assigned to secure the computer systems. The systems were dismantled and taken to the police department. Contents of system directories were listed and the systems were backed up prior to any checking.

Charges for the five arrested persons are pimping, pandering, and conspiracy to commit a crime. The IRS is also investigating the defendants for possible tax evasion violations. At the time of this report, the case had not reached the preliminary hearing stage, and the final adjudication of the defendants is not known.

A primary piece of evidence in the case is, of course, the extensive records maintained on the systems. The prosecutor for this case has stated that the information on the systems will be extremely valuable in proving criminal intent and conspiracy.

Thefts of Hardware/software

Software Piracy

A small business purchased microcomputer hardware and software from a local computer consulting firm. The software consisted of several business applications including modules for accounts receivable, accounts payable, inventory, and customer lists. The software package, which had been developed by a company in Florida, varied in price between $3,000 and $5,000 depending on

the modules purchased. In this case, the total hardware and software cost was about $8,000.

As the small business started using the package, it encountered several problems that could not be answered satisfactorily by representatives of the consulting firm. The small business therefore decided to call the Florida company directly. Upon contact, they were asked to provide the serial number of the software from the floppy disks. Suspicions on the authenticity of the sale were raised at this point since the software had been delivered on the hard disk with no accompanying diskettes.

The small business contacted the CCU, and the unit determined that several other small businesses in the area had purchased the system, including hardware, from the same consulting company. The investigators were able to identify a suspect in the consulting firm and determine that he had been selling the systems through three different companies.

Since all the systems were delivered with the software installed on the hard disks, it was apparent that the proprietary programs had been illegally copied from the original diskettes. The suspect was questioned but denied the allegation. The CCU then requested from the Florida firm all invoices submitted to the companies with which the suspect was associated. These records showed that only one copy of the software had been purchased. When confronted with this information, the suspect admitted to copying the programs and selling the systems. In summary, one copy of the software had been purchased and was being resold along with hardware to several companies.

The suspect was charged with grand theft and was found guilty. He was required to pay full restitution to the software publishing company, plus a two-year suspended sentence, $4,000 fine and court costs, and four years supervised probation.

Other aspects of this case were:

- The software publishing company was reluctant to prosecute because of previous cases that had failed and the fact that they were located in a different state.
- A background check of the perpetrator revealed a history of arrests for various types of frauds. Now he had moved into frauds involving microcomputers—in effect, he had changed with the times.
- The contracts the businesses had signed were poorly written. As a result, a prosecutorial complication in the case was that the suspect had delivered on what he was obligated to do.
- Because the investigation took several months, much of the evidence (pirated software) had been deleted or replaced by the Florida firm. The destruction of the evidence hampered the prosecution of the case.

- The Florida firm was the victim in this criminal case, not the businesses that purchased the software. Because of the successful criminal prosecution, the businesses decided to bring civil actions against the perpetrator. This litigation is currently pending in civil court.

Theft of Silicon Wafers

Silicon wafers are the primary building blocks in computer integrated circuits, so called "computer chips." The victim in this case was an international firm that specialized in chip manufacturing. Their warehouse usually contained several hundred thousand dollars worth of these silicon wafers.

When the international firm decided to move its operations to another state, it was approached by a smaller firm to purchase the wafers. The sale was, however, not culminated. At this point, several employees from the two companies held a secret meeting and decided to steal some of the wafers from the warehouse and sell them through the gray market. Wafers were loaded from the warehouse to a tractor trailer and moved to another location. The international firm did not even realize that a theft had occurred.

The availability of the wafers was then advertised in computer trade catalogs. Purchasing agents from the international firm noticed the advertisements and were curious not only because the product description was identical to their own, but also because no other company could have had the quantity of items described. Their curiosity led to the discovery of the theft, and the CCU was notified.

With the assistance of the international firm, the investigators decided to pose as potential buyers and contacted the employees through the bulletin board. A meeting was then arranged in which $100,000 worth of wafers were purchased.

At the time of this report, one employee had been arrested and charged with grand theft. The final outcome of this arrest has not been determined. Unfortunately, most of the stolen wafers were not recovered and were presumed to have been sold.

Theft of Trade Secrets

This case involved the theft of valuable developmental software by a former employee who had been fired by the company because of incompetence. Before leaving, she obtained the telephone number for accessing the company's computer system. Unfortunately, the company did not delete her password from the system after she left. Over several days, she accessed the system and copied the entire database to her personal computer – an operation taking about 26 hours. Potential value of the information was estimated at more than one million dollars.

The company became suspicious when the system crashed for no apparent reason during daily production reports. While investigating the cause of the problem, it was discovered that several system files had been deleted. In an effort to trace the problem, the staff decided to review the system logs to try to determine when the deletions had occurred. Entries in the log showed system activities at unusual times, such as early morning hours. On the basis of this information, the company notified the CCU which set up a trap and trace on the telephone line into the system. The trace identified the phone of the former employee.

A search warrant was obtained and the search revealed the application software on the suspect's personal computer. In addition, $300,000 worth of stolen software from another company where the employee had worked was also found.

The suspect was charged with several counts of unlawful access to a computer system and theft of trade secrets. This case had not been decided at the time of this report.

Lessons Learned from Local Cases

Several generalizations can be made based on the cases handled by the units participating in this study.

Computer crimes can occur anywhere

Virtually all of the cases discussed in this chapter could have taken place anywhere in the country. They are not germane to the geographical areas in which these CCU's are located. With the proliferation of microcomputers for personal and business use, the opportunities for computer crimes have increased tremendously. A major problem, of course, is that these crimes are not being reported to the police. As discussed in Chapter 2, the reporting levels have increased significantly in the jurisdictions having these units. Their workloads have increased to the point that formal criteria have been established to limit the types of computer crimes they investigate and prosecute.

Who commits computer crimes

The characteristics of the persons committing these offenses depend on the type of computer crime. Hacking and phreaking cases are generally committed by juveniles and young adults. These individuals are usually males who are bored by school work, not socially outgoing, and have few outside activities. They frequently view their actions as a game and see no harm in beating a large company. As one prosecutor put it, they do not know the difference between "Pacman and Pac Bell."

Disgruntled employees commit many internal computer crimes and thefts. These employees may have no other distinguishing features than overtly display-

ing their displeasure with the company. They frequently destroy files with their motive being revenge rather than financial gain. One of their initial questions asked by CCU investigators is about unhappy employees or recently released employees who may have been in a position to commit the crime.

An interesting trend observed by the local investigators is that individuals with previous convictions for frauds are being drawn to computer crimes. In two of the fraud cases discussed in this chapter, the offenders had prior convictions for fraudulent schemes. In essence, these persons are merely applying their experience and skills to a different type of illegal activity.

As in the past, many embezzlements are committed by *opportunists* who take advantage of their positions of trust and authority to commit an offense. These individuals rarely have prior arrest records and are not "hardened" criminals. Local investigators find that these individuals quickly admit to their offenses when confronted.

Computer crime cases require extensive investigative and prosecution time

As stated in Chapter 2, the caseloads of computer crime units are lower than other investigative units. The primary reason is that these cases take a considerable amount of time to develop.

Telecommunications crimes are particularly complex. These cases may extend into several jurisdictions and even into other states. They always involve common carriers and local telephone companies which must be individually contacted for assistance. The investigators find that this assistance is not always easy to obtain since the company may not be the actual victim and the request may be time consuming to fulfill.

Internal computer crime cases are also very time consuming. While these cases do not occur with great frequency, the preparation time by prosecutors can be extensive. The Trojan horse case discussed in this chapter required months of time on the part of the lead prosecutor in the case.

Good coordination between investigators and prosecutors is essential

Because of the technical nature of these cases, it is important for investigators and prosecutors to coordinate their activities. In all the sites, one prosecutor was designated to handle computer crime cases. The standard procedure was for the investigators to meet with this prosecutor early in the case for guidance. Failure to take this initial step can lead to eventual dismissal of the case.

Search warrants are important in obtaining evidence for computer crime cases

In most respects, search and seizure issues in computer cases are like those in other criminal cases. The Fourth Amendment requires that warrants be based on probable cause, supported by oath or affirmation, and issued by an independent judicial officer. Probable cause for a search warrant refers to a

reasonable belief that particular objects or kinds of objects will be found in the place to be searched.

The difficult issues in computer crime cases are twofold: (1) How does the officer applying for the warrant describe what he or she is looking for? (2) What are the limits upon what a searching officer can seize?

The answer to the first question rests mostly in the description of the suspected crime. If the crime is adequately described, the application for a warrant can reasonably use generic descriptions of the instruments, fruits, and evidence of the crime likely to be found in the place to be searched. The application can state that the search is for computers and related equipment, supporting documentation, printouts, code books, and the like without specifying manufacturer, models, specific programs and the like.

The limits on the scope of a seizure are more problematic. Computer disks and diskettes have such large storage capacities that they can easily contain a great deal of information that has nothing to do with the subject matter of the investigation. A particularly troublesome example is the storage of the suspect data on a computer system belonging to someone who has no connection with the crime being investigated, such as an accounting firm that keeps records for the suspect on a hard disk with the records of hundreds of other persons.

Further complications can arise when suspects have taken security measures designed not simply to protect the contents of their files, but to destroy them when an unauthorized user tries to access them. Outside expertise may be needed in conducting the search, particularly when the type of system has not been determined in advance.

There are no ready answers to these problems. Appendix C contains a search warrant written for a computer crime investigation. It at least gives the reader an example of how some investigators have tackled these issues.

Computer crime charges should always be included when there is reasonable evidence that computer crimes have occurred

Depending on the type of case, the computer crime charges may or may not be the primary prosecutorial focus. With internal computer crimes, for example, the computer crime charges are the main charge without question. However, even with embezzlements, the local investigators believe that computer crime charges should always be placed against the suspected offender when there is reasonable belief that computer crimes have been committed. In Baltimore County, for example, a charge of embezzlement from a financial institution will usually be accompanied with charges for illegal access to a computer and misuse of a computer system.

There are several reasons for including computer crime charges with other offenses. First, the CCU should receive credit in these arrests for having

sufficient evidence to include these charges. Secondly, the prosecutor may be able to make good use of these charges in the plea bargaining process. Finally, the computer charges will create an awareness for the judges as to the significance of these offenses.

Chapter 4

Computer Crime Legislation

Introduction

To a lawyer, a crime is whatever the legislature says is a crime. Within the last decade, 48 of the 50 state legislatures and the United States Congress have passed some form of computer crime statute, and most of this chapter will be devoted to consideration of those statutes. But before reaching the statutes themselves, we will briefly set forth some underlying issues of judicial construction and then review some of the earlier computer crime cases. With this background, we will be better able to understand the issues legislatures had in mind drafting their computer crime statutes.

One further introductory point. The computer crime cases decided before there were applicable computer crime statutes and the computer crime statutes themselves provide a further basis for understanding the more recent cases discussed in Chapter 3.

Strict Construction of Criminal Statutes

The Constitutional concept of due process of law, expressed in the Fifth and Fourteenth Amendments of the United States Constitution, requires that everyone be put on clear notice that certain acts are criminal acts. This means that legislatures are to state, in terms understandable by the ordinary person, exactly what they intend to compel or prohibit. As we shall see, this matter of terms is one to which a great deal of attention has been paid in computer crime legislation, but anyone examining the definitions adopted would find it hard to say that they are readily understandable by the ordinary person.

A basic principle of judicial construction is that criminal statutes are strictly construed against the state and in favor of the individual. That is, courts will not interpret a statute liberally or broadly to cover the circumstances of a particular case, as they sometimes do in civil litigation, to achieve what the legislature probably had in mind but failed to express with precision and clarity. Courts will not expand criminal statutes to cover acts the legislature probably would have forbidden had it thought of them. Thus, more often than not, strict construction works for defendants in criminal cases.

Finally, a criminal offense consists of certain specific elements, all of which the prosecutor must prove. For example, larceny at common law was taking and carrying away the personal goods of another of any value, with felonious intent to steal it. That definition breaks down into four elements to be proved: (1) taking, (2) carrying away, (3) goods of another, (4) intent to deprive the owner

of possession permanently. We have chosen larceny as an example because it has often been used as the charge against computer criminals where there was not a computer crime statute. Defenses usually raised include that nothing has been "carried away," the allegedly stolen data or computer program having remained on the computer; or that "property" means only "tangible property," and that electronic impulses are not tangible. These defenses have not often prevailed, but computer crime statutes focus prosecution more on the real problem and not on these tangential issues.

Computer Crime Cases

Computer crime was not going unpunished before the recent proliferation of computer crime statutes. Virtually every computer crime violates laws other than computer crime laws themselves, and prosecutors have successfully prosecuted cases for embezzlement, larceny, fraud, and, in federal courts, for wire fraud and mail fraud. But there have been some problems applying older forms to newer offenses, and specifically designed computer crime statutes should alleviate these problems. Civil litigants have also been successful against computer criminals, and because most state computer crime statutes do not specifically provide for civil relief, civil litigants for the most part will continue to rely on common law or alternative statutory remedies.

Nineteen computer crime cases have been collected in an American Law Reports annotation of an Indiana case.[19] Without going into detailed discussion of these cases, we can make these general observations: (1) Despite some ingenious defense arguments, most courts and prosecutors have had little difficulty applying traditional concepts to computer offenses; (2) federal prosecutors have frequently turned to wire fraud and mail fraud charges where state prosecutors would have charged fraud, larceny, or embezzlement; and (3) courts may refuse to apply traditional definitions to new offenses where there is no readily apparent loss by the victim.

Defenses usually rest on the intangible or incorporeal nature of computer transactions. In a Texas case, the defendant stole 59 computer programs and attempted to sell them to one of his employer's clients for five million dollars. One of his defenses was that computer programs are not corporeal property and therefore not subject to theft. The court noted that the Texas Penal Code section under which the case was brought defines "property," as related to the crime of theft, as including "all writings of every description, provided such property possesses any ascertainable value." It had no trouble finding that computer programs fall within the meaning of that provision.[20] The Alabama Supreme Court reached much the same conclusion in a civil case involving theft of computer payroll programs.[21]

The "intangibility" argument was also unavailing to a federal defendant charged with unauthorized use of property of the United States. He had accessed a NASA computer from his home telephone, using its time and storage capacity

for his own business. He argued that computer time and storage capacity are not "property" or "a thing of value" within the meaning of the statute under which he was being prosecuted, characterizing them as "mere philosophical concepts as distinguished from interests capable of being construed as property." The court rejected the argument:

> The consumption of its time and the utilization of its capacities seem to the court to be inseparable from the physical identity of the computer itself. That the computer is property cannot be questioned. Thus, the uses of the computer and the product of such uses would appear to the court to be a "thing of value" within the meaning of 18 USC § 641, sufficient upon which to predicate a legally sufficient indictment.[22]

A Missouri defendant tried a variation on the intangibility argument.[23] He was charged with stealing by deceit after he used another person's automatic teller card to withdraw $800 in 16 transactions of $50.00 each over a nine-day period. Defendant argued that the indictment failed to state that he had made any representation at all, let alone a fraudulent representation, and failed to state that the bank had acted in reliance on his representations in parting with the $800. The court rejected this argument, saying it was based on the assumption that the misrepresentation had to have been verbal. Actions suffice, and by his actions defendant represented that he had authority to use the other person's bank card and code.

> Just as the facts here show a misrepresentation by defendant through his conduct, so also the facts clearly show reliance thereon by the bank. The machine was so programmed that no money would be paid out without the insertion of the appropriate card and the corresponding personal identification numbers. When those items were supplied, the response was programmed so as to pay out the money. No difference can be perceived whether the bank gave approval after the presentation of those identification items or whether it programmed its acceptance in advance. In either case, the bank equally relied upon the presentation of the card and personal identification.[24]

Several cases illustrate the ease with which federal prosecutors turn computer crime into wire fraud or mail fraud. For example, two TWA employees in Pittsburgh worked a fraud on TWA by keeping and then voiding one-way tickets that had been paid for in cash. They would give the travelers boarding passes and credit transaction receipts, which few people would even notice, let alone question. The two kept the actual ticket, reassembled the ticket packet, and sent it to auditing to be cancelled. Of course, they kept the cash. Part of this transaction entailed printing the ticket, which was done by computer connected to the TWA mainframe in Kansas City. It was this part of the transaction that turned the matter into a federal wire fraud, of which the two were convicted.[25]

In another case, a retail merchant in Brooklyn used counterfeit credit cards to defraud Visa and Mastercard on 267 spurious purchases for over $95,000. Because computerized inquiries to the credit card companies were made on interstate telephone lines, he was found guilty of wire fraud.[26] A third federal case was a mail fraud case in which the mailing was a relatively minor part of the offense, which in all other respects was clearly a computer crime. While working for Sperry Univac's applications development center, defendants developed a system computerizing generation of sheet music. In doing so, they used substantial amounts of computer time and storage capacity within the central processing unit of the applications center development, all without Sperry Univac's knowledge or authorization. In collaboration with another corporation, they agreed to develop and market their sheet music system. The other corporation sent promotional materials through the mail, supplying the basis for the mail fraud prosecution.[27]

There are three cases where lack of a computer crime statute defeated prosecution. *Lund* v. *Commonwealth*[28] led directly to enactment of Virginia's computer crime statute. It is a good example of a court's refusal to stretch old concepts to fit new offenses. Lund was a graduate student in statistics at Virginia Tech who used the university's computer time and services to work on his doctoral thesis, charging the costs back to various departments. He was prosecuted for grand larceny and larceny by false pretense. The Supreme Court of Virginia reversed his conviction. Strictly construing Virginia's larceny statutes, the Court held that computer time and services were not goods and chattels (personal property) within the meaning of the statutes. They could not be carried away. The Virginia General Assembly responded first by amending the larceny statute to include computer time or services,[29] later by enacting a comprehensive computer crime statute.[30]

In *People* v. *Weg*,[31] defendant was a computer programmer for the New York City Board of Education. He was accused of using the Board's computer system to record and retrieve data for his own commercial benefit. More specifically, he was charged with theft of services under New York Penal Code § 165.15(8), which reads:

> Obtaining or having control * * * of business, commercial or industrial equipment or facilities of another person, knowing that he is not entitled to the use thereof, and with intent to deprive a commercial or other substantial benefit for himself or a third person, he uses or diverts to the use of himself or a third person such labor, equipment or facilities.

The court held that the Board of Education's computer was not "business" equipment, both the statutory context and legislative history clearly indicating that the legislature had meant to protect equipment in commercial use. The Board's computer service was not rented or sold to outsiders for a fee.

The court went on to point out that, if the legislature wanted to make unauthorized use of computers a crime, it could do so, as Illinois had done.

> This Court, however, may not create an offense. Unless Penal Law section 165.15(8) is amended, it will apply only to unauthorized tapping into a computer whose service is for hire.[32]

Finally, in *State* v. *McGraw*,[33] McGraw worked for the City of Indianapolis as a computer operator. The City leased computer services on a fixed charge or flat rate basis, so its costs did not vary with the amount of use. McGraw was provided a terminal at his desk and was assigned a portion of the computer's information storage area, called a "private library," for his use in performing his duties.

McGraw became involved in a private sales venture and began soliciting his fellow employees and using a small portion of his assigned library to maintain records. Reprimanded several times for selling his products in the office and on office time, he was eventually fired. After he was fired, McGraw asked a former fellow employee to obtain a printout of his business data and then to erase it from what had been his library. Instead, the printout was turned over to McGraw's former supervisor and became the basis for the criminal charges against him.

McGraw was charged with theft, in that he knowingly exerted "unauthorized control over the property of the City of Indianapolis, Indiana, to wit: the use of computers and computer services with intent to deprive the City of Indianapolis * * *." The Indiana Supreme Court reversed McGraw's conviction because an element of the offense was missing. The Court assumed that McGraw's use of the computer was unauthorized and that such use was "property" under the theft statute. But there was still the question of "deprivation." We quote at length because of the everyday, down-to-earth analogies used by both the defendant and the court:

> * * * Our question is, "Who was deprived of what?"
>
> Not only was there no evidence that the City was ever deprived of any part of the value or the use of the computer by reason of Defendant's conduct, the uncontradicted evidence was to the contrary. The computer was utilized for City business by means of terminals assigned to various employee-operators, including Defendant. The computer processed the data from the various terminals simultaneously, and the limit of its capacity was never reached or likely to have been. The computer service was leased to the City at a fixed charge, and the tapes or discs upon which the imparted data was stored were erasable and reusable. Defendant's unauthorized use cost the City nothing and did not interfere with its use by others. He extracted from the system only such information as he had previously put into it. He did not, for his own benefit, withdraw City data intended for its exclusive use or for sale.

> Thus, Defendant did not deprive the City of the "use of computers and computer services" as the information alleged that he intended to do. We find no distinction between Defendant's use of the City's computer and the use, by a mechanic, of the employer's hammer or a stenographer's use of the employer's typewriter for other than the employer's purpose. Under traditional concepts, the transgression is in the nature of a trespass, a civil matter – and a de minimis one, at that. Defendant has likened his conduct to the use of an employer's empty bookshelf, for the temporary storage of one's personal items, and to the use of an employer's telephone facilities for toll-free calls. The analogies appear to us to be appropriate.[34]

One judge dissented, disagreeing with the majority's conclusion that McGraw did not intend to deprive the City of any property.

> Time and use are at the very core of the value of a computer system. To say that only the information stored in the computer plus the tapes and discs and perhaps the machinery involved in the computer system, are the only elements that can be measured as the value or the property feature of that system, is incorrect.
>
> * * * The fact is the City owned the computer system and all the stations including the defendant's. The time and use of that equipment at that station belonged to the City.[35]

The *Lund*, *Weg*, and *McGraw* cases would all have had different outcomes under computer crime statutes. The court in *Weg* expressly said that the New York legislature could make computer abuse a crime if it chose to, but that it had not so chosen. The Virginia legislature reacted to *Lund* in exactly that way, enacting a computer crime statute.

There is another common thread in these three cases. The courts could well have been resisting imposition of severe penalties in cases where victims had not in fact suffered demonstrable monetary loss. In the computer crime statutes to which we now turn, access without harm is criminalized, although penalties for simple access are usually not harsh.

Computer Crime Statutes

The first state computer crime statute was enacted in Florida in 1978. It became effective on August 1, 1978, and Arizona's statute took effect two months later. Other states soon followed, with 48 now having adopted some form or other of computer crime law. Arkansas was the most recent, in 1987. Only Vermont and West Virginia have not enacted specific computer crime provisions.

As we have seen, except in Virginia, it was not unsuccessful prosecutions under traditional criminal statutes that stimulated this legislative activity. It is hard to

say what did, aside from widespread publicity about potential problems and the absence of any organized opposition. Computer crime in its various forms does not have a constituency. A very interesting analysis of the history of this legislation can be found in an article by Richard C. Hollinger and Lonn Lanza-Kaduce, "The Process of Criminalization: The Case of Computer Crime Laws."[36]

Many states have addressed computer crime in a comprehensive statute, often an independent title in the state criminal code called the "Computer Crimes Act."[37] (See Appendix B for two examples.) At the other extreme, Maine has done nothing more than insert "computer service" as one of the forms of service protected by its Theft of Services provision.[38] Massachusetts has included "electronically processed or stored data, either tangible or intangible," and "data while in transit" in its definition of "property" under its larceny statute.[39]

While many states have created a separate code section for computer crime, many others have placed it in other categories such as Crimes Against Property, Fraud, Theft, Business and Commercial Offenses. Arizona has placed its computer crime provisions under Organized Crime and Fraud, and North Dakota under Racketeer Influenced and Corrupt Organizations (RICO).

We do not want to exaggerate the differences between free-standing computer crime statutes and amendments to existing criminal codes. Some of the former are very brief, targeting specific computer problems, such as unauthorized access or damage to a computer, and leaving other crimes involving computers to be covered by the criminal code as before.[40] On the other hand, California's computer crime provision, which appears as a single section under Crimes Against Property, is quite comprehensive.[41]

There is a philosophical difference between the approaches that deserves comment.[42] With the comprehensive approach, the state legislature creates a new set of definitions and offenses, trying to face the broad array of potential criminal opportunities created by computer technology. There is always a fear that new definitions will give rise to new litigation as courts and litigants shake them down to accepted forms, but that does not seem to have been happening so far with computer crime legislation. Our research on computer crime statutes has turned up no appellate decisions interpreting the new statutes.

The other philosophy is to modify existing law by incorporating new concepts within established forms, thereby minimizing the potential for frustrating the legislative will. Established statutory definitions, approved jury instructions, and judicial precedents can be used. For example, if computer crime is viewed as a form of property crime, then the familiar concepts of property crime can be used in developing and defending cases. The impact of change is alleviated.

There is no one model computer crime statute. The typical computer crime statute will contain the following elements:

- Definitions of terms
- Offenses
- Elements of offenses
- Penalties

Some statutes contain additional provisions:

- Venue
- Civil remedies
- Affirmative defenses

Exhibit 4-1 at the end of this chapter is a summary display of these topics.

Definitions

The definitions set forth in these statutes are always a clear indicator of what problems the legislature is attempting to address. Typically, the following terms will be defined:

- Access
- Computer
- Computer Network
- Computer Program
- Computer Software
- Computer System
- Data
- Financial Instrument
- Property

All the above terms are defined in at least 20 state statutes, and most in over 30. At the other extreme are several terms that appear in only one or two statutes:

- Computer Control Language (Maryland)
- Computer Data Base (Maryland)
- Computer Hacking (South Carolina)
- Computer Supplies (Wisconsin)
- Data Base (New Jersey, Pennsylvania)

- Private Personal Data (Connecticut, Delaware)
- Supporting Documentation (Wisconsin)

These definitions are generally an interesting combination of legal and computer technical styles. Lawyerly words and phrases abound: "including but not limited to," "and any other," "or otherwise," "tangible or intangible," "representation." Computer terms are represented by words like "input," "output," "software," "database," "supporting documentation," "computer network," "computer system."

To illustrate what state legislatures have been doing with definitions, we set forth here Tennessee's definitions, which are typical:[43]

> (1) "Access" means to approach, instruct, communicate with, store data in, retrieve or intercept data from, or otherwise make use of any resources of, a computer, computer system, or computer network;
>
> (2) "Computer" means a device that can perform substantial computation, including numerous arithmetic or logic operations, without intervention by a human operator during the processing of a job;
>
> (3) "Computer network" means a set of two (2) or more computer systems that transmit data over communication circuits connecting them;
>
> (4) "Computer program" means an ordered set of data that are coded instructions or statements that when executed by a computer cause the computer to process data;
>
> (5) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer, computer system, or computer network;
>
> (6) "Computer system" means a set of connected devices including a computer and other devices including, but not limited to, one or more of the following: data input, output, or storage devices, data communication circuits, and operating system computer programs that make the system capable of performing data processing tasks;
>
> (7) "Data" is a representation of information, knowledge, facts, concepts, or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be stored or processed, or is being stored or processed, or has been stored or processed, in a computer, computer system, or computer network;

(8) "Financial instruments" includes, but is not limited to, any check, cashier's check, draft, warrant, money order, certificate of deposit, negotiable instrument, letter of credit, bill of exchange, credit card, debit card, or marketable security, or any computer system representation thereof;

(9) "Intellectual property" includes data, which may be in any form including, but not limited to, computer printouts, magnetic storage media, punched cards, or may be stored internally in the memory of a computer;

(10) "To process" is to use a computer to put data through a systematic sequence of operations for the purpose of producing a specified result;

(11) "Property" includes, but is not limited to, intellectual property, financial instruments, data, computer programs, documentation associated with data, computers, computer systems and computer programs, all in machine-readable or human-readable form, and any tangible or intangible item of value; and

(12) "Services" includes, but is not limited to, the use of a computer, a computer system, a computer network, computer software, computer program, or data to perform tasks.

Several other definitions will be of particular interest to readers of this report. South Carolina defines computer hacking:

(j) "Computer hacking" means accessing all or part of a computer, computer system, or a computer network for the purpose of establishing contact only without the intent to defraud or commit any other crime after such contact is established and without the use of computer-related services except such services as may be incidental to establishing contact.[44]

In a parallel provision, South Carolina makes computer hacking a computer crime in the third degree, a misdemeanor with a maximum $200 fine and thirty days jail for the first offense, but a felony with a maximum $2,000 fine and two years for the second offense.[45] California has a similar provision, but it ups the ante for a second hacking offense to $5,000.[46]

In its first computer crime statute, Illinois defined "electronic bulletin board" and "identification codes/password systems,"[47] but those terms disappeared in a 1987 revision in favor of the terms most frequently seen in the codes of other states, such as "access," "computer," "computer program," and "data."[48]

Offenses

State statutes do not always give computer offenses specific names, and they use a variety of descriptions to state exactly what they are prohibiting. Among the most frequently used titles or descriptions of offenses are the following:

- Access to Defraud
- Access to Obtain Money
- Computer Fraud
- Offenses Against Computer Users
- Offenses Against Intellectual Property
- Offenses Against Computer Equipment and Supplies
- Unauthorized Access
- Unauthorized or Unlawful Computer Use

Defining access offenses is a legislative means of applying common law trespass concepts to computers. In other words, an access offense is usually entering onto someone else's property. If there is no criminal intent beyond curiosity or mischief, then the offense is like South Carolina's computer hacking. But if there is criminal intent, usually to commit a fraud or theft of some kind, then the perpetrator can be prosecuted for both the unauthorized access and the other crime.

There are further wrinkles to access provisions. It is usually specified that interfering with someone else's legitimate access is an offense. Defendants often start out with a right to access, and some states provide for an affirmative defense of authorization, or at least a reasonable belief that access was authorized. Virginia, in a section protecting privacy, draws a line between authorized and unauthorized access, a line that might be easily crossed in an authorized user's search of a database:

> A. A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person. 'Examination' under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.[69]

Unauthorized access is like trespass. Unauthorized taking of computer programs or data is like theft of any other property. In New York, possession of stolen computer programs or data is, in one sense, like possession of any other stolen property, but, in another sense, like possession of a stolen key or a

combination to a safe. Unlawful duplication of computer related material is a felony. Possession of such material, with the intention to benefit someone other than the owner, is a separate felony.[50]

Elements of Computer Crimes

State legislatures have drafted their statutes in very similar, although not identical, ways, so a few examples will suffice to show what specific elements they have included in computer crimes. Virginia provides a compact example of a statute that covers many points in four relatively short sections:

> §18.2-152.3. Computer fraud. – Any person who uses a computer or computer network without authority and with the intent to: (1) Obtain property or services by false pretenses; (2) Embezzle or commit larceny; or (3) Convert the property of another shall be guilty of the crime of computer fraud. * * *
>
> §18.2-152.4. Computer trespass. – Any person who uses a computer or computer network without authority and with the intent to: (1) Temporarily or permanently remove computer data, computer programs or computer software from a computer or computer network; (2) Cause a computer to malfunction regardless of how long the malfunction persists; (3) Alter or erase any computer data, computer programs or computer software; (4) Effect the creation or alteration of a financial instrument or of an electronic transfer of funds; (5) Cause physical injury to the property of another; or (6) Make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs or computer software residing in, communicated by or produced by a computer or computer network shall be guilty of the crime of computer trespass * * *.
>
> §18.2-152.6. Theft of computer services. – Any person who willfully uses a computer or computer network, with intent to obtain computer services without authority, shall be guilty of the crime of theft of computer services * * *.
>
> §18.2-152.7. Personal trespass by computer. – A. A person is guilty of the crime of personal trespass by computer when he uses a computer or computer network without authority and with the intent to cause physical injury to an individual.[51]

We saw another portion of the Virginia statute, Computer Invasion of Privacy, in the previous section.[52]

Virginia uses the term "use" where most other states would say "access." Several of the cases discussed in Chapter 3 are unauthorized access cases, so they are

of particular interest to us. Tennessee provides a typical example of how legislatures have specified the elements of access offenses:[53]

> §39-3-1404. (a) Whoever knowingly and willfully, directly or indirectly, accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof, for the purpose of: (1) Devising or executing any scheme or artifice to defraud; or (2) Obtaining money, property, or services for themselves or another by means of false or fraudulent pretenses, representations, or promises shall, upon conviction thereof, be fined a sum of not more than fifty thousand dollars ($50,000) or imprisoned not less than three (3) nor more than ten (10) years, or both.
>
> (b) Whoever intentionally and without authorization, directly or indirectly accesses, alters, damages, destroys, or attempts to damage or destroy any computer, computer system, or computer network, or any computer software, program or data shall, upon conviction thereof, be fined not more than fifty thousand dollars ($50,000) or imprisoned not less than three (3) nor more than ten (10) years, or both.
>
> (c) Whoever receives, conceals, or uses, or aids another in receiving, concealing or using, any proceeds resulting from a violation of either subsection (a) or (b) of this section, knowing same to be the proceeds of such violation, or whoever receives, conceals, or uses, or aids another in receiving, concealing or using, any books, records, documents, property, financial instrument, computer software, computer program, or other material, property, or objects, knowing same to have been used in violating either subsection (a) or (b) of this section shall, upon conviction thereof, be fined not more than twenty-five thousand dollars ($25,000) or imprisoned not less than three (3) nor more than ten (10) years, or both.

Wisconsin exemplifies another approach, that of focusing completely on the computer without reference to intent to commit some other crime:

> § 943.70 (2) Offenses against computer data and programs.
>
> (a) Whoever wilfully, knowingly and without authorization does any of the following may be penalized as provided in par. (b):
>
> 1. Modifies data, computer programs or supporting documentation.
>
> 2. Destroys data, computer programs or supporting documentation.
>
> 3. Accesses data, computer programs or supporting documentation.

4. Takes possession of data, computer programs or supporting documentation.

5. Copies data, computer programs or supporting documentation.

6. Discloses restricted access codes or other restricted access information to unauthorized persons.

§ 943.70. (3) Offenses against computers, computer equipment or supplies.

(a) Whoever wilfully, knowingly and without authorization does any of the following may be penalized as provided in par. (b):

1. Modifies computer equipment or supplies that are used or intended to be used in a computer, computer system or computer network.

2. Destroys, uses, takes or damages a computer, computer system, computer network or equipment or supplies used or intended to be used in a computer, computer system or computer network.[54]

In Chapter 3, we considered *State of Texas* v. *Burleson*, which was brought under the Texas provision on harmful access:

§ 33.03(B) Harmful Access

(a) A person commits an offense if the person intentionally or knowingly:

(1) causes a computer to malfunction or interrupts the operation of a computer without the effective consent of the owner of the computer or a person authorized to license access to the computer; or

(2) alters, damages, or destroys data or a computer program stored or maintained, or produced by a computer, without the effective consent of the owner or licensee of the data or computer program.[55]

Penalties

Sanctions provided in state computer crime statutes fall roughly into three classes, each of them used by about a third of the states. The overall sanction system of a state's criminal code is of great importance. A third of the states group all sanctions in a separate part of the code, working towards uniformity in sentencing through a systematic classification of crimes and sanctions. In these states, computer crimes will be classified as Class A Felonies, Class B

Felonies, Class C Felonies, Class A Misdemeanors, etc. In such states, the range of penalties and fines will not appear in the computer crime statute itself.

In another third of the states, the penalties are explicitly stated in the computer crime statute. The ranges of fines and sentences are set forth and tied directly to the offenses defined by the statute. Under both these systems, states are penalizing computer crimes at both felony and misdemeanor level. In most states, the maximum penalties will be five years and $25,000, but in Nevada, the fine can be $100,000 and the sentence six years, and in South Carolina, the fine can be $125,000 and the sentence ten years.

The third class of computer crime penalties takes a different, and sometimes problematic, approach. It ties the penalty to the amount of damage or loss suffered by the victim. New Mexico sets five levels of sanctions for computer fraud and unauthorized computer use, depending on the value of the money, property, or services lost:

- Less than $100, petty misdemeanor.
- Between $100 and $250, misdemeanor.
- Between $250 and $2,500, fourth degree felony.
- Between $2,500 and $20,000, third degree felony.
- More than $20,000, second degree felony.[56]

The problem is that such damages are often difficult to measure. Computer services and computer time are bought and sold daily, so arriving at their value should not be difficult. But as we move into proprietary computer uses that are not sold as such, assessing value gets more complex. In a case involving theft of seismic computer programs used in the petroleum industry, an expert witness testified that these programs were worth more than fifty dollars, the statutory minimum required to be proved in the case. He also testified that these programs were worth perhaps as much as two and one-half million dollars.[57] The statutory minimum obviously had no relationship to the true value of the programs.

In *State of Texas* v. *Burleson*, discussed in detail in Chapter 3, the insurance company whose records Burleson had destroyed offered evidence on what it cost to replace and rehabilitate those records.

Connecticut and Delaware empower the court, in lieu of imposing a fine, to sentence the defendant to pay an amount not to exceed double the amount of defendant's gain from the offense. The court may hold a separate hearing on that issue if there is insufficient evidence in the record upon which to base a finding of the defendant's gain.[58] Montana sets the ceiling on a fine at two and one-half times the value of the property used, altered, destroyed, or obtained.[59]

Wisconsin empowers a sentencing judge, in addition to other penalties, to place restrictions on the offender's use of computers. The duration of such a restriction may not exceed the length of time to which the offender could have been sentenced.[60]

Wisconsin is also one of the states that makes special provision for offenses that create "unreasonable risk and high probability of death or great bodily harm to another," making such offenses Class C felonies.[61] Virginia makes "personal trespass by computer," that is, unauthorized use with intent to cause physical injury, a Class 3 felony.[62] Delaware classifies offenses creating "a risk of serious physical injury to another" Class C felonies.[63]

Florida makes offenses against computer equipment or supplies a felony of the second degree "if there is an interruption or impairment of governmental operation or public communication, transportation, or supply of water, gas, or other public service * * *."[64]

Venue

A dozen states include specific venue provisions in their computer crime statutes. Venue refers to the place, that is, the judicial district, in which a case can be prosecuted, which for most crimes is the place where the crime was committed. Venue questions have arisen in computer crime cases because the perpetrator can be at a place quite remote from the place, or places, at which his offense has impact. In a case in which defendants had rigged the Pennsylvania lottery, the offense had impact everywhere in the state where there was a terminal (1400 in all) connected to the lottery. Some of the defendants challenged their prosecution in Harrisburg, claiming that none of the acts that were the basis for the charges had taken place there. The court found from the evidence that the lottery's central computer, without which the rigging could not have taken place, was in Harrisburg and therefore that the offense was committed in Harrisburg.[65]

Venue statutes deal with these problems by making offenses prosecutable in any one of several places. Delaware's statute illustrates the point:

> (a) In any prosecution for any violation of §§ 932-936 of this title, the offense shall be deemed to have been committed in the place in which the act occurred or in which the computer system or part thereof involved in the violation was located.
>
> (b) In any prosecution for any violation of §§ 932-936 of this title based upon more than 1 act in violation thereof, the offense shall be deemed to have been committed in any of the places at which any of the acts occurred or in which a computer system or part thereof involved in a violation was located.

(c) If any act performed in furtherance of the offenses set out in §§932-936 of this title occurs in this State or in any computer system or part thereof accessed in violation of §§ 932-936 of this title is located in this State, the offense shall be deemed to have occurred in this State.[66]

Georgia and Virginia have added provisions pertaining to the computer owner's principal place of business. Georgia's venue provision reads as follows:

For the purpose of venue under this article, any violation of this article shall be considered to have been committed:

(1) In any county in which any act was performed in furtherance of any transaction which violated this article;

(2) In the county of the principal place of business in this state of the owner or lessee of a computer, computer system, computer network, or any part thereof;

(3) In any county in which any violator had control or possession of any proceeds of the violation or of any books, records, documents, property, financial instrument, computer software, computer program, or other material or objects which were used in furtherance of the violation; and

(4) In any county from which, to which, or through which any access to a computer or computer network was made, whether by wires, electromagnetic waves, microwaves, or any other means of communication.[67]

Civil Remedies

Computer crime statutes routinely provide that they are not meant to limit any other provision of civil or criminal codes, leaving the state free to prosecute offenders on other statutory bases, such as fraud or embezzlement, and leaving victims free to pursue their ordinary civil remedies, such as fraud or conversion. Because the level of proof in civil litigation is not as high, and because statutory and common law civil remedies can be broadly construed and shaped to accord relief, there is not the same sense of urgency about providing specific statutory civil remedies for computer crime. But several states have provided such remedies, and it is interesting to note what they have added.

California and Missouri provide compensatory damages, "including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access."[68] The same section of the California Penal Code also provides that "the conduct of an unemancipated

minor shall be imputed to the parent or legal guardian having control or custody of the minor * * *."

Other than the compensatory damage language quoted in the preceding paragraph, civil remedy provisions of computer crime statutes do not say much about how the plaintiff's damages are to be measured. Virginia, however, provides that: "Without limiting the generality of the term, 'damages' shall include loss of profits."[69]

Delaware and Wisconsin provide for injunctions against computer offenses as part of their civil remedies. Wisconsin's statute adds protection against bulletin board activity or other disclosure of confidential passwords or codes:

> In addition, owners, lessors, users or manufacturers of computers, or associations or organizations representing any of those persons, may sue for injunctive relief to prevent or stop the disclosure of information which may enable another person to gain unauthorized access to data, computer programs or supporting documentation.[70]

California, Illinois, Missouri, and New Jersey provide for attorneys' fees. New Jersey allows the award of punitive damages. Delaware has what amounts to a civil forfeiture provision:

> Remedies of aggrieved persons. (a) Any aggrieved person who has reason to believe that any other person has been engaged, is engaged or is about to engage in an alleged violation of any provision of § 932-936 of this title may bring an action against such person and may apply to the Court of Chancery for: (i) An order temporarily or permanently restraining and enjoining the commencement or continuance of such act or acts; (ii) an order directing restitution; or (iii) an order directing the appointment of a receiver. Subject to making due provisions for the rights of innocent persons, a receiver shall have the power to sue for, collect, receive and take into his possession any property which belongs to the person who is alleged to have violated any provision of this subpart and which may have been derived by, been used in or aided in any manner such alleged violation. Such property shall include goods and chattels, rights and credits, money and effects, books, records, documents, papers, choses in action, bills, notes and property of every description including all computer system equipment and data, and including property with which such property has been commingled if it cannot be identified in kind because of such commingling. The receiver shall also have the power to sell, convey and assign all of the foregoing and hold and dispose of the proceeds thereof under the direction of the Court. Any person who has suffered damages as a result of an alleged violation of any provisions of § 932-936 of this title, and submits proof to the satisfaction of the Court that he has in fact been damaged, may

> participate with general creditors in the distribution of the assets to the extent he has sustained out-of-pocket losses. * * *[71]

Two of the cases discussed in Chapter 3 also had parallel civil suits based on the same incidents.

Miscellaneous Features

In addition to features common to the majority of computer crime statutes, there are several that appear in only one or two states but are worth noting. For example, North Carolina has an explicit provision covering extortion:

> Any person who verbally or by a written or printed communication, maliciously threatens to commit an act described in G.S. 14-455 [Damaging computers and related materials] with the intent to extort money or any pecuniary advantage, or with the intent to compel any person to do or refrain from doing any act against his will, is guilty of a Class H felony.[72]

Georgia and Utah create a statutory duty to report computer crimes to law enforcement officials. Georgia's is the more elaborate of the two:

> It is the duty of every business; partnership; college; university; person; state, county, or local governmental agency or department or branch thereof; corporation; or other business entity which has reasonable grounds to believe that a violation of this article has been committed to report promptly the suspected violation to law enforcement authorities. When acting in good faith, such business; partnership; college; university; person; state, county, or local governmental agency or department or branch thereof; corporation; or other business entity shall be immune from any civil liability for such reporting.[73]

Neither Georgia nor Utah provides any sanction for failure to report. It is not clear that these acts create any greater obligation than citizens already have to report crimes.

Washington makes explicit what is left implicit most other places:

> A person who, in the commission of a computer trespass, commits any other crime may be punished for that other crime as well as for the computer trespass and may be prosecuted for each crime separately.[74]

To the extent that other states address this issue, they do so by providing that computer crime provisions are not exclusive and that all other parts of the state code still apply.

In addition to prohibiting unauthorized access to a computer, computer system, or computer network for illicit purposes, Utah makes it a separate offense to allow another person to do the same acts.[75]

Iowa addresses a problem about which most other states remain silent, that of proving what is in a computer. The following provision makes printouts admissible as evidence:

> In a prosecution under this chapter, computer printouts shall be admitted as evidence of any computer software, program, or data contained in or taken from a computer, notwithstanding an applicable rule of evidence to the contrary.[76]

The rule of evidence to the contrary would be the "best evidence rule," which is that the best evidence of the content of a document is the document itself. Iowa's statute eliminates any contention that the printout is only a copy of what is in the computer, not the data that is really there. Best evidence rule arguments hadbeen made in earlier cases.[77]

Virginia specifically provides that a computer can be used as an instrument of forgery,[78] legislatively resolving a definitional problem that had vexed at least two federal courts.[79]

One final note. Oklahoma's statute, reflecting one of that state's principal concerns, includes "geophysical data or the interpretation of that data" in its definition of "property."[80]

Conclusion

Justice Holmes considered the states laboratories for working out a variety of approaches to problems confronting our society. The computer crime statutes we have been considering are an excellent example of what he was talking about. In a very short period of time, short, that is, as far as law-making goes, almost all states have adopted legislation dealing directly and explicitly with computer crime. They have chosen to add these statutes to existing law rather than to substitute them for prior criminal prohibitions and civil remedies, broadening the options available to prosecutors and civil litigants.

These laws are detailed in definition and comprehensive in scope. But if anything characterizes the criminals at whom these laws are aimed, it is their own ingenuity in finding cracks and loopholes in our computer systems and networks. The next decade will show us how good they are at finding flaws in our computer laws.

Exhibit 4-1

Summary of State Statutes

		STATUTORY APPROACH		OFFENSES DEFINED				
	Date Enacted	Computer Crime Act	Amended Criminal Statutes	Unauthorized Access	Computer Fraud	Against Computer Users	Against Computer Systems	Interruption of Services
ALABAMA	1985	◆		◆			◆	
ALASKA	1984		◆	◆				
ARIZONA	1978		◆	◆	◆		◆	
ARKANSAS	1987	◆		◆	◆		◆	
CALIFORNIA	1979		◆	◆	◆		◆	◆
COLORADO	1979	◆		◆	◆		◆	
CONNECTICUT	1984	◆		◆			◆	◆
DELAWARE	1984	◆		◆			◆	◆
FLORIDA	1978	◆		◆	◆	◆	◆	
GEORGIA	1981	◆		◆	◆		◆	
HAWAII	1984	◆		◆	◆		◆	
IDAHO	1984	◆		◆	◆		◆	
ILLINOIS	1979	◆		◆	◆		◆	◆
INDIANA	1986		◆	◆				
IOWA	1984	◆		◆			◆	
KANSAS	1985		◆	◆	◆		◆	
KENTUCKY	1984		◆	◆	◆		◆	
LOUISIANA	1984	◆			◆	◆	◆	
MAINE	1975		◆					
MARYLAND	1984		◆	◆				
MASSACHUSETTS	1983		◆					
MICHIGAN	1979	◆		◆	◆		◆	
MINNESOTA	1982		◆	◆	◆		◆	
MISSISSIPPI	1985	◆			◆	◆	◆	

Exhibit 4-1 (cont.)

	STATUTORY APPROACH			OFFENSES DEFINED				
	Date Enacted	Computer Crime Act	Amended Criminal Statutes	Unauthorized Access	Computer Fraud	Against Computer Users	Against Computer Systems	Interruption of Services
MISSOURI	1982		◆	◆		◆	◆	
MONTANA	1981		◆	◆			◆	
NEBRASKA	1985		◆	◆				◆
NEVADA	1983		◆		◆		◆	◆
NEW HAMPSHIRE	1985		◆	◆			◆	◆
NEW JERSEY	1984	◆		◆	◆		◆	
NEW MEXICO	1979		◆	◆	◆		◆	
NEW YORK	1986	◆		◆				
NORTH CAROLINA	1979	◆		◆	◆	◆	◆	
NORTH DAKOTA	1983		◆	◆	◆			
OHIO	1986		◆					
OKLAHOMA	1984	◆		◆	◆		◆	
OREGON	1985		◆	◆	◆		◆	◆
PENNSYLVANIA	1983		◆	◆	◆		◆	◆
RHODE ISLAND	1979	◆		◆	◆		◆	
SOUTH CAROLINA	1984	◆			◆		◆	
SOUTH DAKOTA	1982		◆	◆	◆		◆	
TENNESSEE	1983	◆		◆	◆		◆	
TEXAS	1985	◆		◆			◆	
UTAH	1979	◆		◆	◆		◆	◆
VERMONT								
VIRGINIA	1984	◆		◆	◆		◆	◆
WASHINGTON	1984		◆	◆			◆	
WEST VIRGINIA								
WISCONSIN	1981		◆	◆	◆		◆	◆
WYOMING	1982	◆		◆	◆	◆	◆	◆

best copy available

Exhibit 4-1 (cont.)

	OFFENSES DEFINED					
	Tampering	Misuse of Information	Theft of Services	Venue	Affirmative Defense	Civil Remedy Provided
ALABAMA			◆			
ALASKA			◆			
ARIZONA						
ARKANSAS				◆		◆
CALIFORNIA			◆	◆	◆	◆
COLORADO						
CONNECTICUT		◆	◆	◆	◆	
DELAWARE		◆	◆	◆		◆
FLORIDA						
GEORGIA				◆		
HAWAII						
IDAHO						
ILLINOIS	◆					
INDIANA	◆					
IOWA			◆			
KANSAS						
KENTUCKY		◆		◆		
LOUISIANA						
MAINE			◆			
MARYLAND						
MASSACHUSETTS			◆			
MICHIGAN						
MINNESOTA			◆			
MISSISSIPPI				◆		

Exhibit 4-1 (cont.)

OFFENSES DEFINED

	Tampering	Misuse of Information	Theft of Services	Venue	Affirmative Defense	Civil Remedy Provided
MISSOURI	◆					◆
MONTANA						
NEBRASKA			◆			
NEVADA						
NEW HAMPSHIRE		◆	◆	◆	◆	
NEW JERSEY	◆	◆		◆		◆
NEW MEXICO						
NEW YORK	◆				◆	
NORTH CAROLINA						
NORTH DAKOTA						
OHIO			◆			
OKLAHOMA						
OREGON			◆			
PENNSYLVANIA		◆				
RHODE ISLAND						
SOUTH CAROLINA				◆		
SOUTH DAKOTA		◆		◆		
TENNESSEE				◆		
TEXAS					◆	
UTAH						
VERMONT						
VIRGINIA			◆	◆		◆
WASHINGTON						
WEST VIRGINIA						
WISCONSIN			◆			◆
WYOMING						

Chapter 5

The Future of Computer Crime

Based on the experiences of the units studied and the trends in the computer industry, we can make educated predictions regarding the future of computer crimes. Increased reporting of computer crimes, more responses by police and prosecutors, and more preventive steps by businesses dominate the trends that are likely to occur.

Reporting Trends

- **Computer crimes will continue to increase and more will be reported to local agencies.**
- **Large companies will be less likely to report computer crimes than small companies.**

It is inevitable that computer crimes of all types will continue to increase. As the number of computers continues to grow for business and personal use, there will be more opportunities for crimes. Internal computer crimes will increase simply because more computers will be used in businesses and more employees will have access to the computers. This access will lead to misuses ranging from minor offenses, such as playing games on a system, to serious destruction of data by disgruntled employees. The loss of data will be one of the greatest fears of businesses and is one reason why more reporting of crimes will occur.

Viruses will also be a great concern to businesses with communications networks. These systems are always susceptible, as reflected in the recent attack on portions of the Defense Department's Internet network. This network is comprised of several national and regional networks, including ARPAnet, which links researchers employed by the Defense Department's Advanced Research Projects Agency, and NSFnet, established by the National Science Foundation to link civilian scientists and engineers. The attack had the effect of bringing computers to a halt and transmitting copies of itself to other computers with the same result.[81] The offender in this case violated federal and state statutes.

Increases in other telecommunications crimes can also be expected. There are approximately 475 long-distance carriers in the United States today. Many of the large carriers are well known, such as MCI and US Sprint. The majority of the other companies are regional, operating in only a few states with a small group of clients. They offer cheaper services to their clients with a limited geographic range. The larger companies are taking steps to improve their security and to prevent crimes on their lines. As they succeed in these efforts,

it can be expected that the small carriers will become victims. This push from large carriers to small carriers will result in more reporting of offenses to state and local law enforcement agencies.

An emerging type of computer crime involves cellular phones. In a recent case in New York City, 18 persons were arrested and charged with having the Electronic Serial Numbers (ESN) and billing numbers in their cellular phones changed. Cases of a similar nature have been reported in California and Florida. In these offenses, valid ESN and billing numbers are stolen and then programmed into the phones. Any calls made with these phones are then charged to innocent persons. Drug dealers have taken advantage of this arrangement to make calls on both a national and international basis.

Hacking and phreaking will continue to appeal to many bright juveniles who enjoy the challenge of breaking into a computer. As security becomes more sophisticated, hacking techniques will also improve.

With regard to who will report computer crimes, our interviews with the participating sites indicate that small businesses will be more likely to report than large companies. There are several reasons for this conclusion. Large companies (over 1,500 employees) are better able to absorb the financial losses from computer crimes. Losses are viewed as a "part of doing business" when the amounts are small relative to total company profits. Further, when loss of data is involved, large companies are more likely to have backup and recovery systems to recreate the files. The result is then a loss of time and inconvenience in establishing the files.

Large companies also frequently have the resources to conduct their own investigations. They may already have an internal security division or they may decide to hire an outside investigator to look into the offense. Even when the offender is found in these cases, an arrest may not be made. Instead, the result is to discharge the employee from the company. From a societal viewpoint, one of the unfortunate consequences is that the offender may obtain a job with another company and commit the same offense. Local investigators have described this situation in their own cases; that is, prior employees of an offender have stated that the person was fired because of committing a computer crime while in their employment.

On the other hand, small businesses may not be able to absorb the loss easily and cannot afford to conduct their own investigations. These businesses will turn to police departments and prosecutors for assistance. They will be more interested in wanting arrests made for the offenses and more likely to press charges.

Investigations by Police Departments and Prosecutors

- **More police and prosecutor agencies will start investigating computer crimes.**
- **There will be more training on computer crimes in police departments and prosecutors' offices.**
- **Agencies will develop high-tech tool kits for investigations.**
- **Computer crime charges will be included more frequently with traditional crimes such as frauds and embezzlements.**
- **Measurements of effectiveness for dedicated units will be developed.**

Because of the increases in reporting, investigators and prosecutors will have to develop ways to address these offenses. Large agencies may establish full-time computer crime units, such as the ones discussed in this report. Other agencies will probably designate an investigator or prosecutor to specialize in these offenses. This person will be called upon whenever the need arises in a case.

Many other arrangements are possible. Police departments may borrow investigators from other departments to conduct and assist in investigations. Virtually all the investigators in the units for this study have been called upon by other agencies in their states and from other states. These requests have ranged from merely checking a microcomputer to assistance in complex investigations. Another arrangement is the development of associations of investigators in a state or region. These associations can then call upon each other for investigations of computer crimes.

Prosecutors' offices offer another alternative for investigating computer crimes. The models offered by Alameda County, California and Tarrant County, Texas may become prevalent in many parts of the country. These two offices have attorneys who specialize in computer crimes as well as in-house investigators who handle computer crime cases and assist surrounding police departments.

The early involvement of prosecutors in these cases has proven particularly beneficial. When the police agencies do not have expertise in computer crimes, the early contacts with prosecutors become even more important. Prosecutors should be able to advise law enforcement agencies on the most appropriate way to proceed in a given case.

Regardless of agency size, police departments and prosecutors' offices will receive more training on computer crimes. While only a few training courses are available now, more courses can be expected in the future. These courses will come in several forms. A few private companies now offer training courses, and more companies can be expected to have courses in the future. Training can also be expected in the form of books and video tapes.

The training needs of police departments can be approached in three overlapping levels:

- All personnel need a general understanding of computer crimes.
- All detectives need an intermediate level of understanding about computer crimes.
- A few detectives need to have extensive training in computer crimes.

The general understanding of computer crimes is obtainable with recruit classes and in-service training. Written materials should be developed providing information on the state statutes pertaining to computer crimes. Officers and supervisory personnel should have a level of understanding about the law in their state. They should be able to identify the elements of computer crimes and should include these charges whenever appropriate in arrests.

Detectives need a higher level of understanding to obtain information on the statutes and on computer systems. It is expected that more cases will involve computers, and detectives will need to know how to take advantage of the information on computers in these cases.

A few investigators should be specially trained in computers and computer crimes. These investigators may become a full-time unit or be assigned to another unit and called upon when needed to assist in computer crimes.

As described in Chapter 2, one of the needs for investigating crimes involving microcomputers is "investigative software." At the present time, this need is being filled by packages available for general use with microcomputers, such as Norton's Utilities and PC Tools. In the future, software specifically tailored to investigations will be available. This "diagnostic" software will allow investigators to check microcomputers in a more efficient manner to determine whether evidence of value exists on the system.

While there may not be a significant increase in the reporting of embezzlements, there should be an increase in computer crime charges associated with embezzlements. It is virtually impossible in a financial institution to commit an embezzlement without also committing a computer crime. These embezzlements usually include unauthorized access to computer systems and misuses of computer systems (by creating fictitious accounts). In the units studied for this report, these charges are always added to the primary embezzlement. As other departments become aware of the statutes on computer crimes, we anticipate that they will also add these charges to the primary charges.

Finally, as dedicated units become established within agencies, the issue of their efforts and effectiveness will arise. The efforts of a unit can be measured in terms of cases handled, arrests, and investigative assists to other units and departments. The traditional effectiveness measure of conviction rates obviously is applicable to computer crime units, and high rates of conviction should be

expected from these units. The value of computer crime evidence in other types of cases should also be measured, even if subjective judgments have to be made.

As with other investigative units, the dedicated units for computer crimes should also have a deterrent effect. However, measuring this effect in any quantitative manner may not be possible. For example, the publicity associated with arrests of hackers is believed by investigators to have an impact on other offenders, but the number of offenders who cease their activities and the volume of these activities cannot be determined. In addition, the speeches at business and security association meetings should result in security changes by businesses. However, there is no way of knowing the range of improvements or the deterrence value of the changes. It may be beneficial, however, for the units to develop case studies of their efforts as a surrogate measure of deterrence effectiveness.

Prevention of Computer Crimes

- **More businesses will take preventive measures to protect their systems.**
- **Commercial software to monitor systems will become popular.**
- **Changes in the workplace discipline will occur to improve security.**

Businesses are the primary victims of computer crimes. They will continue to take preventive measures such as the following to protect their systems:

- Improved methods for authentication of users and terminals (port protection).
- Improved network security software.
- Virus detection software.
- Improved hardware and software for backups.
- Improved disaster recovery planning techniques.
- Anti-theft and identification devices for computer hardware.
- Improved physical protection of hardware to prevent theft.
- Improved entrance control systems into computer areas.

Software programs already exist for monitoring systems. For example, large mainframe systems include a system log which records user access information, such as account name, password, logon time, and logoff time. Variations of these programs record programs and databases accessed during a session.

More sophisticated software is currently being developed. SRI International is developing an Intrusion Device Expert System (IDES) to monitor computer systems for unusual activity. For example, the normal pattern for a user may be between 9:00 a.m. and 5:00 p.m. on weekdays. The system will recognize this

pattern and may not allow access by the user at odd times such as early morning hours.

In the past, there has been a reluctance to include these protective procedures on systems. Their major drawback is that they are "overhead" which take more memory and may decrease the response time of the system. However, with the increases in computer crimes, this reluctance will be put aside in favor of more protection of valuable assets.

Finally, changes in the workplace environment will occur for improved security measures. Lists of accounts and other important information will be shredded rather than discarded in wastepaper baskets. Regulations will be enforced to prevent the appearance of log-on procedures, including passwords, on the sides of terminals or in desk drawers. In summary, computer work areas will have to be kept cleaner as a preventive measure.

Response of Computer Crime Offenders

- **Persons committing computer crimes will use password and encryption methods to protect their systems.**
- **Some defense attorneys will start specializing in computer crimes.**

It cannot be expected that offenders will sit idly while the criminal justice system improves its capabilities in computer crimes. Offenders will take steps to make arrests and convictions more difficult. Two specific ways will be password and encryption methods on systems and the hiring of defense attorneys who specialize in computer crimes.

As a general trend, password and encryption procedures will become more popular with many computer systems. With encryption packages, files can be coded so that a printout of the file is unintelligible. Encryption procedures generally include a password provided by the user, and the file can be decrypted only by knowing the password. Computer crime offenders will take advantage of the packages, making it more difficult to check a computer and obtain information from it.

Some defense attorneys will specialize in computer crime law and will pose a challenge to prosecutors in demonstrating guilt beyond a reasonable doubt. Discovery motions and motions challenging technical points will be the rule, rather than the exception, in these complex cases. Trials will become more frequent, and judges and juries will be called upon to understand the computer terms, analogies, flowcharts, and other tools employed by the attorneys. Computer crime law will be no different than other specialized areas where defendants can turn to attorneys who have become intimately acquainted with the computer crime statutes and can provide a high caliber of legal representation to the defendants.

Conclusions

The experiences of the last 20 years offer an interesting lesson on the impact of a technological change on society. Improvements in computers and telecommunications have altered how people conduct their daily activities and how businesses conduct their transactions. Computers have become such an important aspect of society that legislation has been enacted in virtually every state to protect information vital to the effective use of computers and to ensure that computers are not misused.

The legislation anticipated that jurisdictions would develop effective ways for enforcement and prosecution, but the responses to date have been mixed. As reported here, some localities have established dedicated units aimed at preventing, investigating, and prosecuting computer crimes. However, the predominant reaction has been one of little or no action. The problem exists and legislation provides for sanctions, but the enforcement and prosecution are not always present. The experiences of the nine dedicated units described in this report may prove valuable to others as they consider alternatives in this important area.

References

1. August Bequai. *Technocrimes: The Computerization of Crime and Terrorism*. Lexington Books (D.C. Heath and Company, Lexington, Mass., 1987).

2. "Business Survey: More For Your Money" by Parker Hodges (*Datamation*, April 1, 1988). Results of their 1988 Datamation Budget Survey of 700 business managers.

3. "At Home in the Office" by Margaret Ambry (*American Demographics*, December 1988).

4. "Organizing for Computer Crime Investigation and Prosecution" by Catherine H. Conly, Abt Associates, Cambridge, Massachusetts, 1989.

5. *Computer Crime: Criminal Justice Resource Manual* by Donn B. Parker, Stanford Research Institute, Menlo Park, California (1989).

6. Many other definitions of computer crime exist. In *Computer Crime: Criminal Justice Resource Manual* (Donn B. Parker, SRI International, 1989), computer crime is defined as "any illegal act for which knowledge of computer technology is essential for successful investigation and prosecution." This definition is appropriate for the *Resource Manual* since its aim is to describe how to investigate and prosecute computer crimes. Our definition emphasizes the commission of the crime to reflect the offenses that law enforcement agencies and prosecutors must now investigate.

7. Other authors prefer the term "computer-related crime" to describe illegal acts involving computers. Also appearing in the literature are terms such as "information crime," "computer abuse," "computer fraud," and "telecommunications crimes" to emphasize different aspects of computer crimes.

8. There are at least a dozen electronic "color boxes" in existence for avoiding long-distance charges. A Red Box simulates the pulsed beeps produced when coins are dropped into a pay phone. A Blue Box makes the telephone system believe a hang-up has occurred when, in fact, the line to the destination is still open. A Black Box eliminates the off-hook current to stop the billing but still permits enough current to allow talking. Other boxes include a Purple Box (combines the functions of Red and Blue Boxes), Silver Box (allows the user to tap anyone's line but cannot be used for talking), and Green Box (returns coins to a person calling from a phone booth).

9. "How Business Battles Computer Crime" by Susan Whitchurst (Security Magazine, October 1986). The magazine mailed 1,000 questionnaires to a random sample of its subscribers who buy security products and services. In the 1986 survey, 296 questionnaires were returned for a 40 percent response rate.

10. Report on Computer Crime. Task Force on Computer Crime Section of Criminal Justice American Bar Association (Washington, D.C., 1984).

11. A computer is defined in this section as "an electronic, mag-

netic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."

12. Computer Crime: Criminal Justice Resource Manual by Donn B. Parker, Stanford Research Institute (now SRI International), 1979, p. 129.

13. See "Organizing for Computer Crime Investigation and Prosecution," by Catherine H. Conly, Abt Associates, 1989.

14. To reiterate a point made in the previous chapter, the response of most law enforcement agencies and prosecutors' offices has been to provide training to agency personnel rather than to establish a specialized unit. The advantages and disadvantages of specialized units are discussed at the end of this chapter.

15. For more information on this type of approach, see "Organizing for Computer Crime Investigation and Prosecution" by Catherine H. Conly, Abt Associates, Cambridge, Massachusetts (1989).

16. For further information on available training courses, see "Organizing for Computer Crime Investigation and Prosecution" by Catherine Conly, Abt Associates, 1989.

17. Mr. Burleson initially sued the company for wrongful dismissal, but then dropped the suit. The company's lawsuit came after Mr. Burleson's actions.

18. A Dial Number Recorder (DNR) is a device that can be placed on a telephone line to record information about each call placed from that line. Recorded information includes the telephone number being called, time the call was made, and time the call was completed. Another investigative technique is a "trap" which is used to determine the originating telephone number of a call. Long-distance carriers can place DNRs and traps on telephone lines in order to protect their assets.

19. *State* v. *McGraw*, 480 N.E.2d 552, 51 A.L.R.4th 963 (Ind. 1985), ANNOTATION: Criminal liability for theft of, interference with, or unauthorized use of, computer programs, files, or systems, 51 A.L.R.4th 971. This collection is of cases that have been published in case reporting systems, primarily the regional reporters of the West Publishing Company. There undoubtedly have been many other cases in which there was no reported opinion of the court.

20. *Hancock* v. *State*, 402 S.W.2d 906, 18 A.L.R.3d 1113 (Tex. Crim. App. 1966).

21. *National Surety Corp.* v. *Applied Systems*, 418 So.2d 847 (Ala. 1982).

22. *United States* v. *Sampson*, 6 Comp.L.Serv.Rep. 879 (N.D.Cal. 1978).

23. *State* v. *Hamm*, 569 S.W.2d 289 (Mo.App. 1978).

24. 569 S.W.2d at 291.

25. *United States* v. *Giovengo*, 637 F.2d 941 (3rd Cir. 1980), cert.

den., 450 U.S. 1032, 101 S.Ct. 1743, 68 L.Ed.2d 228.

26. *United States* v. *Muni*, 668 F.2d 87 (2nd Cir. 1981).

27. *United States* v. *Kelly*, 507 F.Supp. 495 (E.D.Pa. 1981).

28. 217 Va. 688, 232 S.E.2d 745 (1977).

29. *See Evans* v. *Commonwealth*, 226 Va. 292, 308 S.E.2d 126 (1983).

30. Va. Code §§ 18.2-152.1 thru 18.2-152.14. For full text, see Appendix B.

31. 113 Misc.2d 1017, 450 N.Y.S.2d 957 (N.Y.City Crim. Ct. 1982).

32. 450 N.Y.S.2d at 961.

33. 480 N.E.2d 552, 51 A.L.R.4th 963 (Ind. 1985).

34. 480 N.E.2d at 554.

35. 480 N.E.2d at 555.

36. *Criminology*, 26:101 (1988).

37. E.g., *see* Alabama Computer Crime Act, Ala. Code 13-A-8-100 to 103; Florida Computer Crimes Act, Fla. Stat. 815.02; Illinois Computer Crime Prevention Law, Ill. Rev. Stat., ch. 38, §§ 16D-1 to 16D-7.

38. 17A M.R.S.A.§ 357(3).

39. M.G.L.A. c. 266, § 30(2).

40. E.g., see Minn. Stat. §§ 609.88, 609.89.

41. California Penal Code, § 502.

42. This point was emphasized to us by a Senior Deputy Prosecuting Attorney from the State of Washington, who participated in writing his state's computer crime provisions, which he refers to as one of the "modification" statutes.

43. Tenn. Code § 39-3-1403.

44. S.C. Code § 16-16-10 (j).

45. S.C. Code § 16-16-20 (4).

46. Cal. Penal Code § 502 (d)(3)(B).

47. Ill. Rev. Stat., § 16-9.

48. Ill. Rev. Stat., ch. 38, §§ 16D-2.

49. Va. Code § 18.2-152-5.

50. N.Y. Penal Code §§ 156.30, 156.35.

51. Va. Code § 18.2-152-3, 152-4, 152-6, and 152.7.

52. Va. Code § 18.2-152-5.

53. Tenn. Code § 39-3-1404.

54. Wisc. Stat. § 943.70.

55. Tex. Penal Code § 33.03.

56. N.M. Stat. 30-16A-3, A-4.

57. *Hancock* v. *State*, 402 S.W.2d 906, 18 A.L.R.3d 1113 (Tex. Crim. 1966).

58. 1984 Conn. Gen. Stat. Ann. § 53a-257; Del. Code Ann. Title 11, 937 (f).

59. Mont. Code Ann. § 45-6-311 (c)(2) (1983).

60. Wis. Stat. § 943.70 (4).

61. Wis. Stat. § 943.70 (2)(b)(4), (3)(b)(4).

62. Va. Code §18.2-152.7.

63. Del. Code Ann. Title 11, § 937 (c).

64. Fla. Stat. § 815.05 (2)(b)(3).

65. *Com.* v. *Katsafanas*, 464 A.2d 1270 (Pa. Super. 1983).

66. Delaware Code Title 11, § 938.

67. Georgia Code § 16-9-94.

68. California Penal Code § 502 (e)(1); Missouri Code § 537.525 is almost identical in its wording.

69. Va. Code § 18.2-152.12.

70. Wisconsin Code § 943.70 (5).

71. Delaware Code Title 11, § 939 (a).

72. N.C. Gen. Stat. § 14-457.

73. Ga. Code § 16-9-95.

74. Wash. Rev. Ann. Code § 9A.52.130.

75.Utah Code Ann. § 76-6-703 (3).

76. Iowa Code Ann. § 716A.16.

77. See *Hancock* v. *State*, 402 S.W.2d 906, 18 A.L.R.3d 1113 (Tex. Crim. App. 1966).

78. Va. Code 18.2-152.14.

79. *United States* v. *Jones*, 553 F.2d 351 (4th Cir. 1977), cert. den., 431 U.S. 968, 97 S.Ct. 2928, 53 L.Ed.2d 1064.

80. Okla. Stat. Ann. § 1952 (7).

81. The program behind this attack was not a true virus since it did not attach itself to other programs. Instead, it is classified as a worm which can create independent, self-contained copies of itself. This worm's only apparent purpose was to reproduce, since it caused no damage to files or programs.

Bibliography

American Bar Association. *Report on Computer Crime*. Chicago: American Bar Association, 1984.

Anonymous. *Computer Security Handbook: The Practitioner's Bible*. Northborough, Massachusetts: Computer Security Institute, 1987.

Anonymous. *1988 Computer Security Buyer's Guide*. Northborough Massachusetts: Computer Security Institute, 1988.

Arkin, Stanley S. ed. *Prevention and Prosecution of Computer and High Technology Crime*. Oakland, California: Matthew Bender, 1988.

Bequai, August. *Technocrimes*. Lexington, Massachusetts: D.C. Heath and Company, 1987.

Bequai, August. *How to Prevent Computer Crime: A Guide for Managers*. New York: John Wiley and Sons, 1983.

Carroll, John M. *Computer Security*. Boston, Massachusetts: Butterworths, 1987.

Conly, Catherine H. "Organizing for Computer Crime Investigation and Prosecution." Cambridge, Massachusetts: Abt Associates, 1989.

Conser, James A., Louis P. Carsone, and Robert Snyder. "Investigating Computer-Related Crimes Involving Small Computer Systems." In Michael Palmiotto, ed. *Critical Issues in Computer Investigations*. 2nd edition. Cincinnati, Ohio: Anderson Publishing Company, 1988.

Cooper, J.A. *Computer-Security Technology*. Lexington, Massachusetts: D.C. Heath and Company, 1984.

Francis, Dorothy B. *Computer Crime*. New York: E.P. Dutton, 1987.

Gallery, Shari Mendelson. ed. *Computer Security: Readings From Security Management Magazine*. Boston: Butterworths, 1987.

Hollinger, Richard C. and Lonn Lanza-Kaduce. "The Process of Criminalization: The Case of Computer Crime Laws." *Criminology*. 26(1): 101.

Ingraham, Donald G. "On Charging Computer Crime." *Computer/Law Journal*. 2: 429-439.

Kusserow, Richard P. *Computer-Related Fraud and Abuse In Government Agencies*. U.S. Department of Health and Human Services, June 1983.

Kutz, Robin K. "Computer Crime in Virginia." *William and Mary Law Review*. 27(783): 783-831.

Landreth, Bill. *Out of the Inner Circle. A Hacker's Guide to Computer Security*. Bellevue, Washington: Microsoft Press, 1985.

Parker, Donn B. *Computer Crime: Criminal Justice Resource Manual*. Menlo Park, California: SRI International, 1989.

Parker, Donn B. *Computer Crime: Investigation and Prosecution*. Menlo Park, California: Stanford Research Institute, 1989.

Parker, Donn B. *Computer Crime: Criminal Justice Resource Manual*. Menlo Park, California: Stanford Research Institute, 1979.

Parker, Donn B. *Crime By Computer*. New York: Charles Scribner and Sons, 1976.

Perry, R.L. *Computer Crime*. New York: Franklin Watts, Inc., 1986.

Reimer, Douglas M. "Judicial and Legislative Responses to Computer Crimes." *Insurance Counsel Journal*. (July 1986): 406-430.

Roaché, Jerome Y. "Computer Crime Deterrence." *American Journal of Criminal Law*. 13 (Summer 1986): 391-416.

Rostoker, Michael D. and Robert H. Rines. *Computer Jurisprudence: Legal Responses to the Information Revolution*. New York: Oceana Publications, 1986.

Sieber, Ulrich. *The International Handbook on Computer Crime: Computer-Related Economic Crime and the Infringements of Privacy*. New York: John Wiley and Sons, 1986.

Sloan, Irving J. *The Computer and the Law*. New York: Oceana Publications, 1984.

Southard, Douglas K. "To Catch a Thief: Criminal Law is Catching Up With High Tech's Information Thieves." *California Lawyer*. (December 1986): 23-25.

Task Force on Computer Crime Section of Criminal Justice American Bar Association. *Report on Computer Crime*. Washington, D.C., 1984.

Thackery, Gail. "Problems of Computer Evidence." In *The Practical Prosecutor*. National College of District Attorneys, Houston. Volume 1985 (2): 10-11.

Tien, James M., Ph.D., Thomas F. Rich, and Michael F. Cahn. *Computer Crime: Electronic Fund Transfer Systems Fraud*. Cambridge, Massachusetts: Public Systems Evaluation, Inc., 1985.

U.S. Department of Justice. *Computer Crime: Computer Security Techniques*. Washington, D.C.: U.S. Government Printing Office, 1982.

Waal, P.C. "Keeping Hackers At Bay." *Telecommunication Technology*. 4(2): 46-48.

Whitehurst, Susan. "How Businesses Battle Computer Crime." *Security Magazine*. October 1986.

Appendix A

Sting Operations for Computer Crimes

Sting Operations

Electronic Bulletin Boards

An electronic bulletin board allows for the storage of information which can be retrieved by other systems calling into the board. It is essentially a database maintained by a system that is accessible by others over telephone lines. Most bulletin boards have been created for specific purposes, usually for the exchange of messages and information among parties with common interests. For example, members of computer clubs maintain bulletin boards for communicating with each other between meetings.

Bulletin boards are especially popular among microcomputer users. Establishment of a bulletin board is facilitated by programs that can be purchased or obtained from public domain software. With one of these programs, a user can establish tailored menus for anyone dialing into the board. These menus will usually contain options on information about the board, bulletins, news summaries, personal mail, conferences, and leaving messages.

In addition, most bulletin boards have different levels of access to restrict users from certain parts of the board. The bulletin board owner, usually called the System Operator (SYSOP), personally establishes the authorized access levels for each user and enters this information into the system. Access is determined by having a user provide their name and password when signing on to the system. A telephone line into the system is the only other requirement for establishing a board on a microcomputer.

Access to bulletin boards generally operates along the following lines:

- A user dials into the bulletin board.
- The board responds with a message asking for the person's name and password.
- The board then provides a menu showing the options available to the user.
- The user selects an option and starts interacting with the system.
- During a session, a user typically may read messages, leave messages, download files, upload files, or join a conference.
- The user eventually "quits" the session and hangs up from the board.

While most bulletin boards have been established for legitimate purposes, there are also "pirate" or "elite" boards that contain illegal information or have been established to advance an illegal activity. Security on these boards is tightly controlled by the owners. With these bulletin boards, users usually have to contact the owner directly to obtain a password for access to different levels of

the system. A degree of trust must therefore be established before the owner will allow access to the board, and the owners develop "power" over who can use the system.

Pirate boards have been found with a variety of illegal information on them including the following:

- Stolen credit card account numbers
- Long distance telephone service codes
- Telephone numbers to mainframe computers, including passwords and account numbers
- Procedures for making illegal drugs
- Procedures for making car bombs
- Hacking programs
- Tips on how to break into computer systems
- Schematics for electronic boxes (e.g., black box).

These boards obviously are a threat to communities, and their existence has gained the attention of some police departments.

Sting Operations with Bulletin Boards

The experiences of the Maricopa County, Arizona, Sheriff's Department and the Fremont, California, Police Department are very instructive on how local departments can establish their own bulletin boards and become part of the network with other boards. Members of the Maricopa County Sheriff's Department were the first in the country to establish such a board. Their board resulted in over 50 arrests with the usual charge being telecommunications fraud.

In September, 1985, the Fremont Police Department established a bulletin board for the primary purpose of gathering intelligence on hackers and phreakers in the area. The operation was partially funded by VISA, Inc., with additional support from Wells Fargo Bank, Western Union, Sprint, MCI, and ITT.

After establishing their bulletin board, they advertised it on other boards as the newest "phreak board" in the area. Within the first four days, over 300 calls were received on the board. During the next three months, the board logged over 2,500 calls from 130 regular users. Through the bulletin board, they persuaded these groups that they had stolen or hacked long-distance telephone service codes and credit card account numbers. They were readily accepted and were allowed access to pirate boards in the area.

The board was operated for a total of three months. During that period, over 300 stolen credit card account numbers and long-distance telephone service

codes were recovered. Passwords to many government, educational, and corporate computers were also discovered on other boards.

The operation resulted in the apprehension of eight teenagers in the area who were charged with trafficking in stolen credit card accounts, trafficking in stolen long-distance telephone service codes, and possession of stolen property. Within the next week, seven more teenagers in California and other states were arrested based on information from this operation.

It was estimated that this group had been illegally accessing between ten and fifteen businesses and institutions in California. They were regularly bypassing the security of these systems with stolen phone numbers and access codes. One victim company estimated that it intended to spend $10,000 to improve its security and data integrity procedures. Other victimized businesses were proceeding along the same lines.

Conclusions

There are several reasons for conducting Sting operations of this type. One of the most important is that it provides a proactive method of identifying hackers and phreakers in the area. These groups are particularly hard to find since they operate in closed circles with personal networks developed from friendships.

Another byproduct of these operations is the publicity surrounding the cases. Sting operations result in a considerable amount of attention from the media. The publicity has the effect of closing down other pirate boards in the area. One of the greatest fears of these offenders is that their systems will be taken, and in the Fremont operation over $12,000 of computer equipment was seized. The publicity associated with these seizures seems to be the primary reason for others to stop their pirate boards.

These operations also lead to other types of offenses. In Fremont, for example, drug and alcohol cases were developed as a result of the Sting operation. This has been typical of these operations.

The Sting operations with bulletin boards have been criticized because teenagers, rather than hardened criminals, are arrested. Many hackers believe that they have a right to the data in other systems and that their activities are not illegal since the companies can afford the losses. On the other hand, as one investigator observed, the hackers of today may be the sophisticated computer criminals of tomorrow. It is therefore important to set a lesson early in their careers steering them away from these offenses.

Appendix B

Computer Crime Statutes for Arkansas and Virginia

ARKANSAS

CHAPTER 41

COMPUTER-RELATED CRIMES

SECTION.	SECTION.
5-41-101. Purpose.	5-41-105. Venue of Violations.
5-41-102. Definitions.	5-41-106. Civil actions.
5-41-103. Computer fraud.	5-41-107. Assistance of Attorney General.
5-41-104. Computer trespass.	

5-41-101. Purpose.

It is found and determined that computer-related crime poses a major problem for business and government; that losses for each incident of computer-related crime are potentially astronomical; that the opportunities for computer-related crime in business and government through the introduction of fraudulent records into a computer system, the unauthorized use of computers, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great; that computer-related crime has a direct effect on state commerce; and that, while various forms of computer crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a statute be enacted which deals directly with computer crime.

5-41-102. Definitions.

As used in this chapter, unless the context otherwise requires:
(1) "Access" means to instruct, communicate with, store data in, or retrieve data from a computer, computer system, or computer network;
(2) "Computer" means an electronic device that performs logical, arithmetic, and memory functions by manipulating electronic or magnetic impulses and includes all input, output, processing, storage, computer software, and communication facilities that are connected or related to that device in a system or a network;
(3) "Computer network" means the interconnection of communications lines with a computer through remote terminals or a complex consisting of two (2) or more interconnected computers;
(4) "Computer program" means a set of instructions, statements, or related data that, in actual or modified form, is capable of causing a computer or a computer system to perform specified functions;
(5) "Computer software" means one (1) or more computer programs, existing in any form, or any associated operational procedures, manuals, or other documentation;
(6) "Computer system" means a set of related, connected, or unconnected computers, other devices, and software;

(7) "Data" means any representation of information, knowledge, facts, concepts, or instructions which are being prepared or have been prepared and are intended to be processed or stored, are being processed or stored, or have been processed or stored in a computer, computer network, or computer system;
(8) "Financial instrument" includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computer system representation thereof;
(9) "Property" includes, but is not limited to, financial instruments, data, computer programs, documents associated with computers and computer programs, or copies thereof, whether tangible or intangible, including both human and computer readable data, and data while in transit;
(10) "Services" includes, but is not limited to, the use of a computer, a computer system, a computer network, computer software, a computer program, or data.

5-41-103. Computer fraud.

(a) Any person commits computer fraud who intentionally accesses or causes to be accessed any computer, computer system, computer network, or any part thereof for the purpose of:
(1) Devising or executing any scheme or artifice to defraud or extort; or
(2) Obtaining money, property, or services with false or fraudulent intent, representations, or promises.
(b) Computer fraud is a Class D felony.

5-41-104. Computer trespass.

(a) Any person commits computer trespass who intentionally and without authorization accesses, alters, deletes, damages, destroys, or disrupts any computer, computer system, computer network, computer program, or data.
(b) Computer trespass is a Class C misdemeanor if it is a first violation which does not cause any loss or damage;
(c) Computer trespass is a Class B misdemeanor if:
(1) It is a second or subsequent violation which does not cause any loss or damage; or
(2) It is a violation which causes loss or damage of less than five hundred dollars ($500).
(d) Computer trespass is a Class A misdemeanor if it is a violation which causes loss or damage of five hundred dollars ($500) or more, but less than twenty-five hundred ($2,500).
(e) Computer trespass is a Class D felony if it is a violation which causes loss or damage of two thousand five hundred dollars ($2,500) or more.

5-41-105. Venue of violations.

For the purpose of venue under this chapter, any violation of this chapter shall be considered to have been committed in any county:
(1) In which any act was performed in furtherance of any course of conduct

which violated this chapter;
(2) In which any violator had control or possession of any proceeds of the violation or of any books, records, documents, property, financial instrument, computer software, computer program, data, or other material or objects which were used in furtherance of the violation;
(3) From which, to which, or through which any access to a computer or computer network was made whether by wires, electromagnetic waves, microwaves, or any other means of communication;
(4) In which any computer, computer system, or computer network is an object or an instrument of the violation is located at the time of the alleged violation.

§5-41-106. Civil actions.

(a) Any person whose property or person is injured by reason of a violation of any provision of this chapter may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits.
(b) At the request of any party to an action brought pursuant to this section, the court, in its discretion, may conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer system, computer network, computer program, computer software, and data involved in order to prevent possible reoccurrence of the same or a similar act by another person and to protect any trade secrets of any party.
(c) No civil action under this section may be brought except within three (3) years from the date the alleged violation of this chapter is discovered or should have been discovered by the exercise of reasonable diligence.

5-41-107. Assistance of Attorney General.

If requested to do so by a prosecuting attorney, the Attorney General may assist the prosecuting attorney in the investigation or prosecution of an offense under this chapter or any other offense involving the use of a computer.

CODE OF VIRGINIA

ARTICLE 7.1.

COMPUTER CRIMES.

§ 18.2-152.1 Short title.—This article shall be known and may be cited as the "Virginia Computer Crimes Act."

§ 18.2-152.2. Definitions.—For purposes of this article:

"*Computer*" means an electronic, magnetic, optical, hydraulic or organic device or group of devices which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. The term "computer" includes any connected or directly related device, equipment, or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device.

"*Computer data*" means any representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared and is intended to be processed, is being processed, or has been processed in a computer or computer network. "Computer data" may be in any form, whether readable only by a computer or only by a human or by either, including, but not limited to, computer printouts, magnetic storage media, punched cards, or stored internally in the memory of the computer.

"*Computer network*" means a set of related, remotely connected devices and any communications facilities including more than one computer with the capability to transmit data among them through the communications facilities.

"*Computer operation*" means arithmetic, logical, monitoring, storage or retrieval functions and any combination thereof, and includes, but is not limited to, communication with, storage of data to, or retrieval of data from any device or human hand manipulation of electronic or magnetic impulses. A "computer operation" for a particular computer may also be any function for which that computer was generally designed.

"*Computer program*" means an ordered set of data representing coded instructions or statements that, when executed by a computer, causes the computer to perform one or more computer operations.

"*Computer services*" includes computer time or services or data processing services or information or data stored in connection therewith.

"*Computer software*" means a set of computer programs, procedures and associated documentation concerned with computer data or with the operation of a computer, computer program, or computer network.

"*Financial instrument*" includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security or any

computerized representation thereof.
"*Owner*" means an owner or lessee of a computer or a computer network or an owner, lessee, or licensee of computer data, computer programs, of computer software.

"*Person*" shall include any individual, partnership, association, corporation or joint venture.
"*Property*" shal l include:
1. Real property;
2. Computers and computer networks;
3. Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:
a. Tangible or intangible;
b. In a format readable by humans or by a computer;
c. In transit between computers or within a computer network or between any devices which comprise a computer; or
d. Located on any paper or in any device on which it is stored by a computer or by a human; and
4. Computer services.
A person "*uses*" a computer or computer network when he:
1. Attempts to cause or causes a computer or computer network to perform or to stop performing computer operations;
2. Attempts to cause or causes the withholding or denial of the use of a computer, computer network, computer program, computer data or computer software to another user; or
3. Attempts to cause or causes another person to put false information into a computer.
A person is "*without authority*" when he has no right or permission of the owner to use a computer, or, he uses a computer in a manner exceeding such right or permission.

§ 18.2-152.3. Computer fraud. – Any person who uses a computer or computer network without authority and with the intent to:
1. Obtain property or services by false pretenses;
2. Embezzle or commit larceny; or
3. Convert the property of another shall be guilty of the crime of computer fraud. If the value of the property or services obtained is $200 or more, the crime of computer fraud shall be punishable as a Class 5 felony. Where the value of the property or services obtained is less than $200, the crime of computer fraud shali be punishable as a Class 1 misdemeanor.

§ 18.2-152.4. Computer trespass. – Any person who uses a computer or computer network without authority and with the intent to:
1. Temporarily or permanently remove computer data, computer programs or computer software from a computer or computer network;
2. Cause a computer to malfunction regardless of how long the malfunction persists;

3. Alter or erase any computer data, computer programs or computer software;
4. Effect the creation or alteration of a financial instrument or of an electronic transfer of funds;
5. Cause physical injury to the property of another; or
6. Make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs or computer software residing in, communicated by or produced by a computer or computer network shall be guilty of the crime of computer trespass, which shall be punishable as a Class 1 misdemeanor.

§ 18.2-152.5. Computer invasion of privacy. – A. A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person. "Examination" under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.
B. The crime of computer invasion of privacy shall be punishable as a Class 3 misdemeanor.

§ 18.2-152.6. Theft of computer services. – Any person who willfully uses a computer or computer network, with intent to obtain computer services without authority, shall be guilty of the crime of theft of computer services, which shall be punishable as a Class 1 misdemeanor.

§ 18.2-152.7. Personal trespass by computer. – A. A person is guilty of the crime of personal trespass by computer when he uses a computer or computer network without authority and with the intent to cause physical injury to an individual.
B. If committed maliciously, the crime of personal trespass by computer shall be punishable as a Class 3 felony. If such act be done unlawfully but not maliciously, the crime of personal trespass by computer shall be punishable as a Class 1 misdemeanor

§ 18.2-152.8. Property capable of embezzlement. – For purposes of § 18.3-111, personal property subject to embezzlement shall include:
1. Computers and computer networks;
2. Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:
a. Tangible or intangible;
b. In a format readable by humans or by a computer;
c. In transit between computers or within a computer network or between any devices which comprise a computer; or
d. Located on any paper or in any device on which it is stored by a computer or by a human; and
3. Computer services

§ 18.2-152.9. Limitation of prosecution. – Notwithstanding the provisions of §19.2-8, prosecution of a crime which is punishable as a misdemeanor pursuant to this article must be commenced before the earlier of (i) five years after the commission or the last act in the course of conduct constituting a violation of this article or (ii) one year after the existence of the illegal act and the identity of the offender are discovered by the Commonwealth, by the owner, or by anyone else who is damaged by such violation.

§ 18.2-152.10. Venue for prosecution. – For the purpose of venue under this article, any violation of this article shall be considered to have been committed in any county or city:

1. In which any act was performed in furtherance of any course of conduct which violated this article;
2. In which the owner has his principal place of business in the Commonwealth;
3. In which any offender had control or possession of any proceeds of the violation or of any books, records, documents, property, financial instrument, computer software, computer program, computer data, or other material or objects which were used in furtherance of the violation;
4. From which, to which, or through which any access to a computer or computer network was made whether by wires, electromagnetic waves, microwaves, or any other means of communication;
5. In which the offender resides; or
6. In which any computer which is an object or an instrument of the violation is located at the time of the alleged offense.

§ 18.2-152.11. Article not exclusive. – The provisions of this article shall not be construed to preclude the applicability of any other provision of the criminal law of this Commonwealth which presently applies or may in the future apply to any transaction or course of conduct which violates this article, unless such provision is clearly inconsistent with the terms of this article.

§ 18.2-152.12. Civil relief; damages. – A. Any person whose property or person is injured by reason of a violation of any provision of this article may sue thereof and recover for any damages sustained, and the costs of suit. Without limiting the generality of the term "damages" shall include loss of profits.

B. At the request of any party to an action brought pursuant to this section, the court may, in its discretion, conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer program and computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party.

C. The provisions of this article shall not be construed to limit any person's right to pursue and additional civil remedy otherwise allowed by law.

D. A civil action under this section must be commenced before expiration of the time period prescribed in § 8.01-40.1.

§ 18.2-152.13. Severability. – If any provision or clause of this article or application thereof to any person or circumstances is held to be invalid, such invalidity shall not affect other provisions or applications of this article which can be given effect without the invalid provisions or application, and to this end the provisions of this article are declared to be severable.

§ 18.2-152.14. Computer as instrument of forgery. – The creation, alteration, or deletion of any computer data contained in any computer or computer network, which if done on a tangible document or instrument would constitute forgery under Article 1 (§ 18.2-168 et seq.) of Chapter 6 of this Title, will also be deemed to be forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to any crime set forth in Article 1 (§ 18.2-168 et seq.) of Chapter 6 of this Title if a creation, alteration, or deletion of computer data was involved in lieu of a tangible document or instrument.

Appendix C

Search Warrant
County of Maricopa, State of Arizona

Search Warrant
County of Maricopa, State of Arizona

Warrant No._____

To Any Peace Officer in the State of Arizona:

Proof by affidavit having been made this day to me by _____

_____

I am satisfied that there is probable cause to believe that on the premises known as 9897 Lonesome Road, a single-story residential structure with an attached double carport, block construction, beige with red/brown wood trim, the structure being located on the north side of Lonesome Road facing south, with a desert-landscaped front yard containing a "For Sale" sign, in the City of *Phoenix*, County of *Maricopa*, State of Arizona, there is now being possessed or concealed certain property or things described as:

Computers, central processing units, external drives or external storage equipment or media, terminals or video display units, together with peripheral equipment such as keyboards, modems or acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, electronic tone-generating devices;

Computer software programs, together with instruction manuals and associated documentation;

The following records and documents, whether contained on paper in handwritten, typed, photocopied, or printed form, or stored on computer printouts, magnetic tape, cassettes, disks, diskettes, photo-optical devices, or any other medium: Telephone and communication service billing records, computer, electronic and voice mail system information, access numbers, passwords, personal identification numbers (PINS), telephone and address directories, logs, notes, memoranda and correspondence relating to theft of telephone and communication services, or to unauthorized access into computer, electronic and voice mail systems;

Together with proof of identity, use or ownership of all of the above.

Which property or things

( ) were stolen or embezzled,
( ) were used as a means for committing a public offense,
( ) are being possessed with the intent to use as a means of committing a public offense
( ) are in the possession of _____ for the purpose of concealing it or preventing it from being discovered,

(X) constitute evidence tending to show that a public offense has been committed, or tending to show that a person or persons of unknown identity have committed the offense, such public offense being the crimes of computer fraud (A.R.S. § 13-2316), theft (A.R.S. § 13-1802), telecommunication fraud (A.R.S. § 13-3707),

(*was*) (*is being*) committed by a person or persons unknown residing at 9897 Lonesome Road, Phoenix, Arizona.

You are therefore commanded in the daytime (excluding the time period between 10:00 pm and 6:30 am) to make a search of the above-named or described person(s), premises, or vehicles for the above described property or things, and if you find the same or any part thereof, to retain such in your custody or in the custody of the Arizona Attorney General's office, or Maricopa County Sheriff's office as provided by A.R.S. § 13-3920.

Return this warrant to me within five (5) days of the date thereof, as directed by A.R.S. §§ 13-3918 and 13-3921.

Given under my hand and dated this _____ day of February 1988

_____

Judge

Maricopa County Superior Court

State of Arizona)No._____

)Affidavit for Search

County of Maricopa)Warrant

Affiant, Sgt. William F. Nibouar, is a certified peace officer in the State of Arizona, employed by the Maricopa County Sheriff's office. Based upon the following information, affiant believes there is probable cause for the issuance of a search warrant for the premises known as 9897 Lonesome Road, Phoenix, Arizona.

1. On February 16, 1988, affiant was contacted by R.E. "Sandy" Sandquist, Regional Security Manager, U.S. Sprint Communication Company, 1099 18th Street, Denver, Colorado, who provided the following information:

Since December 1987, Sandquist has been investigating fraudulent use of the Sprint communications system through the computerized switch which services the Phoenix, Arizona area. This fraudulent use of the system has been accomplished by persons whose identities are not yet known, employing stolen

customer authorization codes to place long-distance telephone calls. While the full extent of the losses to U.S. Sprint is not yet known, 8 stolen codes have been identified to date, each with an initial loss of over $1000.

A Sprint customer authorization code is a set of numbers assigned to a specific customer. The code functions as a credit card, enabling the customer to place long-distance telephone calls from any touch-tone telephone. Charges for calls placed are billed to the customer account to which the authorization code is assigned. The customer completes a call by dialing a U.S. Sprint access number such as XXX-XXXX, or 1-800-XXX-XXXX, from a touch-tone telephone. When the connection to the Sprint system is complete, a tone is heard, and the customer then enters the customer authorization code. Without an authorization code, the system will not complete the call.

Sandquist contracted with the Mountain Bell Telephone Company for a trap-and-trace device to be placed on the Sprint system, to identify the originating telephone numbers of suspected fraudulent calls placed through Sprint access numbers. The trap-and-trace revealed that on December 30, 1987, several calls were placed from the telephone number 602-XXXX to the local Sprint access number, 602-XXX-XXXX. This information indicated that someone at that number was placing long-distance telephone calls through the Sprint network. That telephone number was subscribed to by 9897 Lonesome Road, Phoenix, Arizona. Upon investigation, Sandquist was unable to locate any valid account with U.S. Sprint assigned to that telephone number, or to XXXXX.

In November 1987, Sandquist learned of an earlier arrest of several computer hackers by the Mount Lebanon, Pennsylvania, Police Department. Art Kuhn, Special Agent, U.S. Secret Service, informed Sandquist that one of the persons involved in that case had stated that her source of telephone authorization calls was someone who called himself "Doctor No" at telephone number 602-XXXX. This is the same telephone number obtained from the trap-and-trace installed in December.

Sandquist contracted with Mountain Bell for a dialed number recorder (DNR) to be installed on 602-XXXX, and the DNR was attached on January 20, 1988, by Kenneth Nelson, Assistant Staff Manager, Mountain Bell Security. A dialed number recorder captures the electronic impulses travelling over a telephone line as the numbers on a telephone are dialed or pushed. The device records the numbers dialed or pushed on a paper tape for review, but does not record the voice communication.

An initial review of the DNR tapes revealed that 12 long-distance calls were completed through the Sprint network between January 27 and February 10, 1988, from telephone number 602-XXXX, using five different Sprint customer authorization codes. All five codes belong to Sprint customers, and all five accounts have suffered fraudulent charges posted to those accounts by persons not authorized by the customer to use the code. When a code is identified by

Sprint as having been stolen, that code is removed from the system and the legitimate customer is issued a new authorization code. Losses attributable to theft of the code are borne by U.S. Sprint; the customer is not held responsible for unauthorized toll charges.

The DNR also revealed that several other long-distance carriers are being used to place calls from 602-XXXX. MCI access number 602-XXX-XXXX was called 25 times on February 8 and 9, 1988. After checking their records, MCI informed Sandquist that they do not have a customer by the name of XXXX, nor do they have a customer assigned the telephone number 602-XXXX. While the investigation is still continuing, the DNR tapes also indicate use of the Allnet communications network.

Kenneth Nelson also reported that the DNR tapes showed at least 53 calls between January 27 and February 1, 1988, to 1-800-XXX-XXXX, a number subscribed to by Jupiter Manufacturing and Marketing Company, 2319 Maine Avenue, Fairdale, Pennsylvania. A second Jupiter Manufacturing number, 1-800-XXX-XXXX, was dialed 101 times between February 8 and February 11, 1988. Nelson contacted the company, and was informed by John King, Security Representative, Risk Management Department, that these two numbers provide access through several telephone lines into the Jupiter proprietary voice-mail system.

2. Affiant interviewed John King and Alan T. Elias, Manager, Telecommunications Information Systems, both employed by Jupiter Manufacturing. They provided the following information:

The Jupiter voice-mail system allows authorized Jupiter employees to obtain a "voice mailbox" which is capable of performing several functions. Among these are the ability to receive and store messages from callers, to send messages to other boxes on the system, and to send messages to a pre-selected group of boxes. These functions are achieved by pushing the appropriate numerical commands on a telephone keypad for the desired function. To leave a message, the caller dials one of the two "800" numbers listed above, and hears a message identifying the system as the Jupiter Manufacturing and Marketing Company voice-message system. The caller is then instructed to enter the number of the box he wishes to reach. The caller enters a four-digit box number, and hears whatever greeting the box owner has chosen to leave. The caller can exercise several options, one of which is to leave a message after the tone. In this respect, the voice-mail system operates much like a telephone answering machine. Rather than being recorded on audio tape however, the message is stored in digitized form by the computer system. The entire voice-mail system is actually a computer system accessible through telephone lines. The messages are stored on large-capacity computer disks.

An outside caller needs to know only the assigned box number in order to leave a message for a Jupiter employee. In order to retrieve the messages or to delete

them from the system, however, the person to whom the box is assigned must have both the box number and a confidential password-the password ensures privacy of the communications, by acting as a "key" to "unlock" the box and reveal its contents. The employee to whom the box has been assigned also has the ability to change his password, thereby preventing access to the box contents by anyone who may have learned his password.

King and Elias stated that since December 1987, they have been receiving reports from authorized users of abuse of the system. Among the abuses complained of were harassing, obscene, anti-Semitic and threatening messages left in various boxes, and the "taking over" of several boxes by unknown persons who somehow obtained the passwords, gained access to the boxes, then changed the passwords to deny access to the assigned users. In one box, Jupiter proprietary financial data had been left for a Jupiter employee; that box was accessed, and the message contents were disseminated by means of messages left on other stolen boxes.

King and Elias also reported a significant increase in the use of the system during this period. While they do not yet know the full extent of Jupiter's losses, the company pays AT&T the charges for use of their two "800" numbers which provide access into the voice-mail system. In addition, the unauthorized users have interrupted service to Jupiter employees and have occupied a significant portion of the system's available disk storage capacity.

When information obtained from the DNR installed on 602-XXXX was relayed to them, they obtained access to some of the stolen boxes, and heard messages announcing Sprint, MCI, and Allnet authorization codes.

3. For the last three years, affiant has been employed in the Computer Crime Section of the Maricopa County Sheriff's office. During that time, affiant has investigated over 30 cases involving the theft of long-distance telephone services and unauthorized access to computer systems. Affiant has also received training in the investigation of computer fraud and "hacking" (the unauthorized invasion of computer systems by various means) from the International Association of Chiefs of Police and the Federal Bureau of Investigation.

Through his experience, affiant has learned that persons engaged in the theft of long-distance communication services and dissemination of stolen authorization codes commonly employ computer communications devices, computer bulletin boards, and voice-mail systems to facilitate the dissemination of stolen codes and other information. Affiant has found that in virtually all cases, both communications-service abusers and computer hackers maintain either written or computer-stored records of the access numbers, authorization codes, passwords, and other information relating to these activities.

Affiant is also aware that a dialed number recorder, in addition to recording numbers punched or dialed from the telephone facility on which it is installed, records any transmission of the special signaling tones which are used to control

communications networks and their associated automatic billing systems. Through Kenneth Nelson and "Sandy" Sandquist, affiant learned that on more than one occasion, the DNR installed on 602-XXXX recorded the use of the special signaling tone, indicating that that signal had been transmitted from that telephone facility. Through his experience, affiant has learned that the special signaling tone can be generated by an electronic tone-generating device known as a "blue box," or by a personal computer and computer software which enables the computer to generate the tone signal through a communications device (a modem or acoustic coupler) connecting the computer to the telephone line. In his past investigations, affiant has frequently found that persons stealing communications services have possessed a personal computer and the necessary software which would allow them to manipulate communications networks by means of the special signaling tones.

4. R.E. "Sandy" Sandquist stated that for the last four years, he has been employed full-time by GTE and Sprint to investigate telecommunications fraud. He stated that in 1987, he investigated over a half-dozen cases in which search warrants were executed, and in every one of these cases, records were found which related to the theft of services. In each case in which the special signaling tones (or "blue box" tones) had been used, a computer with tone-generating software was found.

Based upon all of the foregoing, affiant believes that probable cause exists for the issuance of a search warrant for the residence located at 9897 Lonesome Road, Phoenix, Arizona.

_____
William F. Nibouar, Sergeant
Maricopa County Sheriff's Office

Subscribed to and sworn before me this _____ day of _____ 1988.

_____
Judge, Maricopa County
Superior Court

Appendix D

Discovery Materials

Discovery Materials

Motion for Discovery, Production, and

Inspection of Evidence

The following are needed for purposes of discovery:

I. A Copy of the NON-system save which was done on or about 9/18/85 *and* on or about 9/21/85.

A. The NON-system Save (or NON-SYS) is like a carbon copy of what was on the computer at the time it was saved. This "NON-SYS" is written on magnetic tape. This particular "NON-SYS" consisted of about 12 reels of magnetic tape on *each* of the days in question (or about 24 tapes total). The Complainant normally did a "NON-SYS" two times a week on Sunday and Wednesday. In addition, they normally did a "SAVCHGOBJ" (a daily save/copy to magnetic tape of any objects which had changed since the last "NON-SYS" save).

B. Items needed from the "NON-SYS" save are copies of Program Source Files and/or machine objects. In particular the following source files are needed from *all libraries* on the "NON-SYS": QDDSSRC (source file containing file layouts), QCLSRC (source file containing Command Language Programs), QRPGSRC (source file containing documentation and/or other textual materials in English language form), QUDSSRC (source files containing Data File Utility {DFU} and Query {QRY} programs), QCMDSRC (source file containing Command Source). Each "library" (a designated storage "compartment") will/should have each of the source files listed above.

C. Reason Needed: Previously obtained documentation and testimony indicate that a program which allegedly deleted records from the Complainants' computer system was similar to a "machine object" found in the Defendant's test library and that it was the only one like it in the system. The defendant would like to have expert witnesses examine the objects and sources involved.

D. Since this material has been under "complete and sole" control of the complainant, any denial of this request for discovery would deny due process to the defendant and his right to examine the evidence against

him and have independent testimony regarding the nature of the complainant's claims.

E. It should be noted that this material is written onto the tape at 6250 BPI (bits per inch) and is a considerable quantity of "data." Any other media will be too difficult to manage and would require an unnecessary burden on the complainant for compliance. The defendant is not interested in any data files per se except those which were allegedly damaged by the deletion of records. The defendant has already filed an affidavit of non-disclosure.

II. A copy of the Save Changed Objects which was done on or about 9/16/85 *and* 9/17/85.

III. A *copy of the Object Dump* and a *copy of the program object* of the program which was used in the deletion of records from file(s) involved. A copy of the source listing of the RPG program which deleted records.

IV. A copy of the following QHST logs (QHST logs are logs of "events" taking place on the computer system. These are automatically generated by the computer for certain and various "events." They show, for example, which persons/user profiles signed onto the machine, the time of sign on, the device at which the sign on occurred, and other similar type "events.") The complainant has already supplied some QHST logs, but these are needed in addition to those previously supplied. These are also saved on magnetic tape:

QHST85261A

QHST85262A

QHST85263A

QHST85264A

QHST85265A

QHST85266A

QHST85267A

QHST85268A

QHST85269A

QHST85270A

Criminal District Court

Inventory of Items Requested by Defendant

To the Honorable Judge of Said Court:

Now comes the state of Texas, by and through her criminal district attorney, and files this inventory of items requested for inspection by Defendant.

Copies of the below listed documents are contained in the State's Case file of the above styled and numbered cause and are available for inspection by Defendant and His Attorney at a time to be set by the Court, or during the normal working hours of the District Attorney's office.

1) Untitled Flow-chart charting involved programs.
2) Object dump: CMRSS.
3) Object dump: CMRCSR.
4) Source listing: ARCARF.
5) Object dump: ARCARF.
6) Template of ARCARF.
7) Object dump: Q$DDCMG.
8) Object dump: URCARF.
9) Object dump: DRCSMR.
10) Object dump: DRCSMRI.
11) Object description for DMRMMR.
    Object dump for : CMRCSWR.
12) Compile listing of CMRCSWR.
13) Object dump: URCARFS.
    Object dump: ARCTM2.
14) Source listing for URCARFS.
    Object dump for: EXTTYP.
15) Source listing: ARCARFARF.
16) Object dump: ARCARFARF.

17) Source listing: CORDNETDU.

18) Source listing: QCLSRCKLD.

Object dump: DMRJNEKDY.

Object dump: CORDNETDO.

19) Object dump: ARRARF.

20) Data Area: ARAARF.

21) Program source listing: DLTRREC.

22) Source listing: DLTCREC.

23) Partial member listing: QRPGSRC.

24) Library Size Analysis Report,
dated "09/24/85."

25) Partial library list of library: DGB.

26) Object description display: DMRJNEKDY.

Object description display: DMRMMRC.

Object description display: DRCSMR.

Object description display: DRCSMRI.

Object description display: EXTTYP.

Object description display: Q$DDCMG.

Object description display: URCARF.

Object description display: URCARFS.

Object description display: ARAARF.

27) Various Object description display.

28) List of Objections with Creation Date in
September. (15 documents)

29) List of objects with a creation date equal to
9/21/85 or 9/03-04/85. (5 documents)

30) List of programs created at DGB.

31) Job logs.

32) Manual down time logs.

33) Manual system logs: April 20, 1985 through March 21, 1986.

36) QHST log 85241A.

37) QHST log 85244A.

38) QHST log 85246A.

End of Inventory.

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

Washington, D.C. 20531

Official Business
Penalty for Private Use $300

BULK RATE
POSTAGE & FEES PAID
DOJ/NIJ
Permit No. G-91